

Department of Motor Vehicles:

Although Unable to Measure the Extent of Identity Fraud and the Effect of Recent Reforms, It Should Improve Its Technology, Procedures, and Staffing Further



September 2001
2001-103

The first five copies of each California State Auditor report are free. Additional copies are \$3 each, payable by check or money order. You can obtain reports by contacting the Bureau of State Audits at the following address:

**California State Auditor
Bureau of State Audits
555 Capitol Mall, Suite 300
Sacramento, California 95814
(916) 445-0255 or TDD (916) 445-0255 x 216**

OR

**This report may also be available
on the World Wide Web
<http://www.bsa.ca.gov/bsa/>**

The California State Auditor is pleased to announce the availability of an online subscription service. For information on how to subscribe, please visit our Web site at www.bsa.ca.gov/bsa. If you need additional information, please contact David Madrigal at (916) 445-0255, ext. 201.

Alternate format reports available upon request.

Permission is granted to reproduce reports.



CALIFORNIA STATE AUDITOR

ELAINE M. HOWLE
STATE AUDITOR

STEVEN M. HENDRICKSON
CHIEF DEPUTY STATE AUDITOR

September 27, 2001

2001-103

The Governor of California
President pro Tempore of the Senate
Speaker of the Assembly
State Capitol
Sacramento, California 95814

Dear Governor and Legislative Leaders:

As requested by the Joint Legislative Audit Committee, the Bureau of State Audits presents its audit report concerning whether the Department of Motor Vehicles' (Motor Vehicles) procedures for issuing driver licenses and its resources are adequate to detect or prevent the issuance of fraudulent documents.

This report concludes that a major weakness in Motor Vehicles' ability to crack down on identity fraud is that it cannot use the computer-mapped finger images (finger images) it collects to verify the identity of all applicants for driver licenses and identification cards (ID cards). Although Motor Vehicles has been collecting finger images for roughly 20 years, it lacks the benefit of technology that would allow it to use them to verify the identity of all its customers. Motor Vehicles has taken important steps to reduce the issuance of fraudulent driver licenses and ID cards; however, it cannot accurately quantify the effect of its new procedures and additional improvements are needed. For example, the photos that are retrieved for existing customers obtaining any temporary license, driver license, or ID card are not verified by a second employee. Also, Motor Vehicles has not taken steps to evaluate and implement most of the recommendations of its Anti-Fraud Task Force.

Finally, Motor Vehicles' investigation of potential fraud also has room for improvement. For example, its Field Investigations Branch lacks procedures dictating how staff should manage and resolve complaints. As a result, Motor Vehicles is unable to accurately determine how long its cases remain open and justify what its true staffing needs are. Further, Motor Vehicles has not established a clear policy that precisely identifies the role of the Special Investigations Branch in investigating employee misconduct and therefore cannot ensure that it investigates all questionable employee activities or that employees participating in these activities receive consistent discipline.

Respectfully submitted,

ELAINE M. HOWLE
State Auditor

BUREAU OF STATE AUDITS

CONTENTS

<i>Summary</i>	1
<i>Introduction</i>	7
<i>Chapter 1</i>	
More Can Be Done to Help Motor Vehicles Prevent Driver License and Identification Card Fraud	13
Recommendations	34
<i>Chapter 2</i>	
The Investigations and Audits Division Needs Better Policies, Procedures, and More Staff to Effectively Resolve Fraud Complaints	37
Recommendations	46
<i>Response to the Audit</i>	
Business, Transportation and Housing Agency Department of Motor Vehicles	49
<i>California State Auditor's Comments on the Response From the Department of Motor Vehicles</i>	65

SUMMARY

Audit Highlights . . .

Our review of the Department of Motor Vehicles (Motor Vehicles) to determine whether it has adequate procedures and resources to detect or prevent the issuance of fraudulent documents revealed that:

- Motor Vehicles lacks the technology to use the computer-mapped finger images it collects to verify the identity of all applicants for driver licenses and ID cards.*
 - Motor Vehicles cannot accurately quantify the effect of new procedures aimed at detecting or reducing fraud.*
 - Motor Vehicles can implement further procedures such as requiring two employees to verify photos it retrieves for existing customers obtaining a temporary license, driver license, or ID card.*
 - Motor Vehicles can better help employees prevent fraud by standardizing its fraudulent document detection training course.*
 - Motor Vehicles' Investigations and Audits Division, responsible for investigating fraud, lacks adequate policies, procedures, and resources.*
-

RESULTS IN BRIEF

By issuing driver licenses and identification cards (ID cards)—California's basic identification documents—the Department of Motor Vehicles (Motor Vehicles) enables residents to establish who they are for the purposes of driving, getting jobs, and making basic financial transactions such as purchasing goods and opening lines of credit. In the past year, Motor Vehicles issued about 8 million driver licenses and ID cards, with an unknown number of them going to people who managed to outwit the issuing system and obtain fraudulent driver licenses or ID cards. Some Motor Vehicles customers commit identity theft by taking over someone else's personal information and "becoming" that person on a driver license or ID card.

Although hard to quantify, the public cost of identity theft and other forms of driver license and ID card fraud can be considerable. Responding to national concerns about increased identity theft, Motor Vehicles recently implemented reforms that strengthen its safeguards against fraud. These reforms are reasonable and may reduce fraud, but further changes are required to better secure the process by which California residents and workers obtain their basic identification documents.

A major weakness in Motor Vehicles' ability to crack down on identity fraud is that it cannot use the computer-mapped finger images (finger images) it collects to verify the identity of all applicants for driver licenses and ID cards. Widely accepted by the public and by law enforcement communities as a reliable means of human recognition, current finger-imaging technology allows a highly accurate electronic comparison of the person at the counter with all other persons in a database system. Unfortunately, Motor Vehicles does not obtain the benefits of such technology. Although it has collected finger images for roughly 20 years, image quality may be poor, and Motor Vehicles lacks the up-to-date hardware and software needed to make this human-recognition method effective and useful.

Last year, when Motor Vehicles sought funds to upgrade its finger-imaging technology, the Legislature denied the request, despite its past support for cutting down on identity theft and

other similar crimes. Although the legislative record is unclear on why the request was denied, according to the Legislative Analyst's Office *Analysis of the 2001–02 Budget Bill*, Motor Vehicles did not sufficiently develop its request, address employee oversight issues, or consider the potential impacts on privacy and efficiency. In light of the reforms Motor Vehicles has recently implemented and the need to further strengthen processes for issuing driver licenses and ID cards, the Legislature may again have to consider whether it believes finger imaging is a more effective means of combating fraud. If the Legislature does approve funding to allow Motor Vehicles to upgrade its system, Motor Vehicles should work with the Legislature to craft laws that address privacy concerns by restricting the uses of and access to finger-imaging data.

To try to prevent issuing fraudulent driver licenses and ID cards, Motor Vehicles has begun verifying Social Security numbers with the federal Social Security Administration, retrieving renewal customers' most recent photographs from the Motor Vehicles database, and requiring two employees to verify birth-date and legal-presence documents that customers present to obtain original licenses. However, Motor Vehicles cannot accurately quantify the effect of its new procedures for three reasons. First, Motor Vehicles has inadequate methods of tracking potential fraud. Second, changes in the way Motor Vehicles categorizes and investigates fraud make it difficult to compare the number of potential fraud cases identified before and after the new procedures were in place. Third, the effect reforms have on deterring attempts to obtain fraudulent driver licenses or ID cards is impossible to measure.

Although increased controls should help prevent fraud, Motor Vehicles could improve on its recent reforms. For example, a second employee does not verify the photo retrieved for an existing customer obtaining a temporary license, driver license, or ID card. Motor Vehicles believes that this poses minimal risk because there is no evidence of employees helping someone assume an identity through fraudulent photo verification. Although Motor Vehicles does not have any data to support this position, it states that it will consider having its Driver License Fraud Analysis Unit (Fraud Analysis) select a sample of new photos of customers requesting duplicate or renewal driver licenses and compare them to prior photos to determine whether it is the same person.

Our review of Motor Vehicles' procedures for issuing driver licenses and ID cards suggests additional internal controls that would reduce fraud. We found, for instance, that Motor Vehicles needs to ensure employees enter bar-code numbers for all requests supported by paper applications and then send the applications to headquarters for microfilming. Bar-code numbers allow Motor Vehicles to electronically track the microfilm location of the application. Employees must consistently follow these procedures to facilitate a new electronic process Motor Vehicles is working on to reconcile paper applications with computer requests for driver licenses and ID cards. Also, Motor Vehicles has yet to evaluate or implement most of the recommendations of its Anti-Fraud Task Force (task force). Finally, since the new fraud prevention procedures have increased the average waiting times of customers with appointments by 1.5 minutes and customers without appointments by 9.3 minutes, Motor Vehicles needs to continue its efforts to improve customer service and mitigate this effect.

Another way Motor Vehicles helps its employees prevent fraud is by offering a training course in fraudulent document detection. However, a lack of uniformity among the trainers' presentations and not enough hands-on experience with original documents are examples of the shortcomings of this training. Course developers state that they need increased funding for trainer education and course materials.

Motor Vehicles' investigation of potential fraud also has room for improvement. Its Investigations and Audits Division (Investigations), responsible for preventing and investigating fraud, lacks adequate policies, procedures, and resources. We found the following weaknesses in Investigations' various branches:

- The Field Investigations Branch (Field Investigations) lacks procedures for managing and resolving complaints, so staff use varying methods to record a complaint's open and close dates in its case management database. Additionally, the database does not account for any time that other units, such as Fraud Analysis, may have held the cases. As a result, Motor Vehicles is unable to accurately determine how long its cases remain open and what its true staffing needs are.
- A flawed database prevents staff in Field Investigations' 30 offices from sharing information such as current fraud trends.

- Fraud Analysis, which analyzes finger images, photos, and fraudulent documents, lacks sufficient staff to handle an increased workload caused by Motor Vehicles' new fraud prevention procedures and consumer fraud hotline.
- Because it has not precisely defined the role of the Special Investigations Branch (Special Investigations) in investigating employee misconduct, Motor Vehicles cannot ensure that it investigates all questionable employee activities or that it imposes consistent disciplinary action against employees participating in these activities.

Motor Vehicles recognizes that deficiencies in staffing, procedures, and technology limit how well it can meet existing goals and effect necessary improvements to reduce fraud. Motor Vehicles is presently reviewing its infrastructure needs and defining its future goals.

RECOMMENDATIONS

If current reforms to the process for issuing driver licenses and ID cards prove insufficient, the Legislature should reconsider funding an upgrade of Motor Vehicles' finger-imaging technology. If it provides the funds, the Legislature should consider protecting against unauthorized dissemination of finger images by allowing only those entities it believes have a legitimate interest in protecting the public, such as state and local law enforcement agencies, to access Motor Vehicles' finger-imaging data. The Legislature should also consider imposing criminal sanctions for unauthorized use of the data. Further, if the Legislature approves the use of finger imaging, it should consider directing Motor Vehicles to establish controls that protect the privacy of California citizens.

To further improve its existing controls and reduce the time customers must wait in field offices, Motor Vehicles should take these actions:

- Establish mechanisms to track the effectiveness of its recent and future reforms.
- Instruct Fraud Analysis to conduct a study to determine the benefits of comparing the new photo of an existing customer obtaining a temporary license, driver license, or ID card with photos contained in the Motor Vehicles database.

- Continue to work on its plan to electronically reconcile system transactions against applications sent for microfilming at headquarters to ensure that an application supports each transaction. Further, field office managers should ensure that field representatives enter bar-code numbers for all paper applications before sending them to headquarters.
- Establish deadlines for staff to address all of the task force recommendations and conduct a timely evaluation of the merits of each recommendation.
- Continue to communicate with trainers and supervisors regarding Motor Vehicles' commitment to standardization and uniformity in its fraudulent document detection training. Determine if Investigations needs additional funding to improve its training program.
- Complete a staffing analysis to assess the impact of recent reforms on Motor Vehicles' ability to carry out its procedures.

To increase its effectiveness in stopping fraud, assisting victims, and helping to prosecute wrongdoers, Investigations should take these actions:

- Establish complaint management procedures that include, at a minimum, logging in a complaint on receipt, promptly sending out an acknowledgment letter to the complainant, prioritizing and assigning complaints, and deadlines for completing the investigation and reporting the results.
- Evaluate the staffing needs of its branches and units.
- Establish a clear policy that identifies Special Investigations' role in investigating employee misconduct; defines such misconduct; and clarifies how employees, managers, and regional administrators should report employee misconduct.

AGENCY COMMENTS

Motor Vehicles agrees with all of the recommendations contained in our report. In fact, it has already begun implementing some of our recommendations. ■

Blank page inserted for reproduction purposes only.

INTRODUCTION

BACKGROUND

Established in 1915, the Department of Motor Vehicles (Motor Vehicles) falls under the authority of the Business, Transportation and Housing Agency. Motor Vehicles employs about 9,300 people, with the majority (almost 4,900) working throughout the State in the 170 field offices that issue driver licenses and identification cards (ID cards). Issuing these documents is one of Motor Vehicles' primary responsibilities to people who live or work in California. As Table 1 shows, Motor Vehicles issued roughly 6.7 million driver licenses and 1.3 million ID cards in fiscal year 2000–01.

TABLE 1

Driver Licenses and ID Cards Issued in Fiscal Year 2000–01

	Driver Licenses	ID Cards
Original	890,909	717,508
Renewal	4,407,396	628,615
Duplicate	1,419,687	N/A*
Totals	6,717,992	1,346,123

Source: Motor Vehicles' Driver License Issuance Activities Report for July 2000 through June 2001.

Note: As of July 10, 2001, Motor Vehicles had more than 24 million driver licenses and ID cards outstanding.

* All ID cards Motor Vehicles issues are either originals or renewals.

For fiscal year 2000–01, Motor Vehicles generated revenue of about \$139 million from issuing driver licenses and ID cards, which are the basic documents that people in California use to establish identity when they drive, get jobs, or make purchases. Because they contain personal information such as name, address, birth date, and physical description, these documents allow an identity thief to perpetrate fraud by co-opting some piece of an individual's personal information without that person's knowledge. An identity thief may open new credit-card or bank accounts in an individual's name and may use those accounts to run up charges without paying the bills or to write

bad checks. A victim's losses may include not only out-of-pocket financial losses but additional costs associated with trying to restore his or her reputation in the community and correcting erroneous information for which the criminal is responsible.

Motor Vehicles' Field Operations Division has a major responsibility to prevent fraud because its 4,000 field representatives are typically the first stop for customers applying for driver licenses and ID cards. In the process of issuing new and renewal driver licenses and ID cards, field representatives verify the authenticity of documents customers present to establish their identities and use equipment to capture and store a customer's finger, photo, and signature images in the Motor Vehicles database.

Other Motor Vehicles divisions also have responsibilities in detecting and preventing driver license and ID card fraud. For example, the Investigations and Audits Division (Investigations) investigates criminal driver license fraud by both the public and Motor Vehicles employees. Table 2 shows the responsibilities of other Motor Vehicles divisions that help prevent fraud.

TABLE 2

Other Motor Vehicles Divisions That Detect and Prevent Fraud

Division	Branch or Unit	Responsibilities
Licensing Operations	Driver Licensing Branch	Issues driver licenses and ID cards and safeguards the integrity and security of the information in the driver license database.
Administrative Services	Departmental Training Branch	Develops and delivers training for Motor Vehicles employees and maintains training records.
Investigations and Audits	Field Investigations Branch	Investigates criminal activity of individuals trying to obtain fraudulent driver licenses or ID cards.
	Special Investigations Branch	Investigates instances and allegations of employee crime, including theft and issuing fraudulent driver licenses or ID cards.
	Electronic Oversight Branch	Uses automated techniques to monitor for fraudulent and unauthorized transactions originating from Motor Vehicles employees and customers.
	Driver License Fraud Analysis Unit	Analyzes possible fraudulent documents and transactions, responds to fraud hotline calls, and tracks crime trends.
	Driver License Investigative Support Unit	Aids field investigators and Driver License Fraud Analysis Unit technicians.

Identity theft is difficult to track because it is an element of many crimes and cuts across the statistical categories tracked by law enforcement agencies. Although the driver licenses and ID cards that Motor Vehicles issues are the basic identification documents in California, it is hard to estimate how much identity theft relies on these documents. Motor Vehicles is only aware of potential fraud that is brought to its attention through the complaints it receives. For example, between November 2000 and August 2001, Motor Vehicles told us that it received about 12,000 complaints from customers, law enforcement agencies, and other public and private entities.

In a report issued last year, Motor Vehicles estimated that its Driver License Fraud Analysis and Driver License Investigative Support units annually handle about 2,400 cases for individuals stating they are victims of identity theft. To make this estimate, Motor Vehicles kept a log of all phone calls and correspondence it received for almost one month and found that 8.8 percent of the incoming cases were from individuals claiming to be victims of financial fraud, such as having checking accounts or lines of credit opened in their names. Motor Vehicles then applied this percentage to the roughly 27,500 complaints it handles annually. However, Motor Vehicles' approach of using less than one month's worth of data to project an annual figure is unsound. Specifically, for extrapolation to be reliable, the composition of the incoming cases must be consistent from month to month.

SCOPE AND METHODOLOGY

The Joint Legislative Audit Committee (audit committee) requested the Bureau of State Audits to determine if the procedures Motor Vehicles uses to issue driver licenses are adequate to detect or prevent the issuance of fraudulent documents. We also reviewed Motor Vehicles' process for issuing ID cards, because the procedures are similar to those it uses to issue driver licenses. The audit committee also asked us to do the following:

- Determine if Motor Vehicles employees are following departmental procedures.
- Determine the effectiveness of Motor Vehicles' recent reforms.
- Examine Motor Vehicles' monitoring of its employees' activities.

- Determine whether Motor Vehicles has sufficient resources and uses these resources to detect or prevent the issuance of fraudulent driver licenses.
- Assess Motor Vehicles' procedures for investigating reports of fraudulent driver licenses.

To understand Motor Vehicles' process for issuing driver licenses and ID cards as well as its recent reforms, we reviewed relevant state laws, regulations, policies, and procedures. In addition, we conducted various interviews with Motor Vehicles staff, union representatives, and a representative from the Legislative Analyst's Office.

To determine whether employees are following the recent procedures established to prevent the issuance of fraudulent driver licenses and ID cards, we evaluated the role and responsibilities of the regional offices that oversee field offices and visited 20 field offices. To make sure that our sample included a representative number of field offices in each region throughout the state, we analyzed the following data:

- The number of driver license and ID card applications marked as potentially fraudulent.
- The number of employee investigations.
- Driver license and ID card transaction volume.
- Staff-to-supervisor ratios.

During our visits, we interviewed employees, managers, and customers. Further, we observed field representatives processing driver license and ID card transactions.

To evaluate how effectively Motor Vehicles trained its staff to identify legitimate birth-date and legal-presence documents, we conducted interviews with employees who participated in Motor Vehicles' training for fraudulent document detection, reviewed evaluations of the training, assessed the lesson plan, and attended a training session. We also reviewed the databases Motor Vehicles uses to track employees who attend the course.

During our audit, we found that the recent reforms increased customer waiting times. To determine what action Motor Vehicles has taken to alleviate customer waiting times, we reviewed documentation on its queuing and online appointment systems. We also conducted interviews with employees and customers to assess the effectiveness of the queuing system.

Our evaluation of whether Motor Vehicles adequately uses its resources to prevent and detect the issuance of fraudulent driver licenses and ID cards included the following procedures:

- To understand why Motor Vehicles does not use the finger images it has been collecting for roughly 20 years to more effectively verify the identity of its customers, we interviewed Motor Vehicles staff and reviewed state law, court cases, progress made on a pilot study regarding the quality of Motor Vehicles' existing finger images, and other literature discussing the pros and cons of finger imaging.
- To determine the role and responsibilities of Investigations and the adequacy of its efforts to prevent and detect the issuance of fraudulent driver licenses and ID cards and employee fraud, we reviewed its policy and procedures manual, analyzed staffing and caseload levels, and conducted interviews with division personnel. We also reviewed a sample of case files to analyze the accuracy of Field Investigations' case management database.
- To further examine controls over its employees' activities, we evaluated the adequacy of Motor Vehicles' pre-employment screening process, reviewed its database for monitoring employee background checks, and examined personnel files. We also reviewed the recommendations of the Director's Advisory Committee on Employee Crime and the Anti-Fraud Task Force, which suggest ways to prevent fraud by Motor Vehicles employees and by the public. Both entities are composed of Motor Vehicles employees, law enforcement personnel, and private industry experts.

Finally, Motor Vehicles is presently analyzing its infrastructure needs and defining its future goals. The results of these efforts will be reported in its Five-Year Infrastructure Plan and Blueprint for the Future. However, because these plans are in the early stages of development, we could not evaluate them. ■

Blank page inserted for reproduction purposes only.

CHAPTER 1

More Can Be Done to Help Motor Vehicles Prevent Driver License and Identification Card Fraud

CHAPTER SUMMARY

Because the documents it issues allow people in California to prove who they are when driving, obtaining bank loans and credit lines, and cashing checks, the Department of Motor Vehicles (Motor Vehicles) must spend considerable time and effort refining its procedures for issuing driver licenses and identification cards (ID cards). The potential for identity fraud requires Motor Vehicles to carefully verify who its customers are. Despite its recent reforms, Motor Vehicles' current technology and training programs limit its ability to meet its responsibility.

Although it collects and stores computer-mapped finger images (finger images), Motor Vehicles cannot use them to verify the identity of customers applying for driver licenses and ID cards. Finger images could greatly reduce the incidence of identity fraud by allowing electronic comparison of images to determine if multiple customers are on one license database record or if one customer has multiple license database records. However, inadequate technology and the possible poor quality of existing images prevent Motor Vehicles from using these data.

During fiscal year 2000–01, Motor Vehicles sought funding to upgrade its technology, but the Legislature denied its request. The Legislature previously supported measures to cut down on identity theft or other similar crimes. Considering the recent reforms Motor Vehicles has implemented to reduce fraud and the additional steps we believe Motor Vehicles should take to strengthen its processes for issuing driver licenses and ID cards, the Legislature may again have to consider whether it believes finger imaging would be a more effective way to combat fraud. If the Legislature does approve additional funding for technology upgrades, Motor Vehicles and the Legislature should work together to craft laws that address the concerns of privacy rights advocates, effectively restricting who can use the data and for what purpose.

Lacking the funding it needs for finger-imaging upgrades, Motor Vehicles has taken other important steps to avoid issuing fraudulent driver licenses and ID cards, including electronically verifying Social Security numbers, retrieving customers' most recent photographs from its database to verify their identity when updating existing records, and requiring secondary verification of birth-date and legal-presence documents when issuing original licenses. These reforms should reduce the incidence of fraud; however, Motor Vehicles is currently unable to measure the impact of its recent reforms. Also, our review shows that Motor Vehicles needs further improvements in its controls to protect the public from identity theft.

Another area of concern is Motor Vehicles' inconsistent training for fraud detection. The goals of division management and field office managers conflict regarding which employees should receive the training, and database flaws prevent the division from knowing if it is even meeting its goals. The fraud detection course needs a better curriculum and improved instructional materials. Additionally, the trainers need to be more qualified and better prepared. Without these improvements, Motor Vehicles cannot use all the tools available to it to help prevent fraud.

MOTOR VEHICLES CANNOT USE EXISTING COMPUTER-MAPPED FINGER IMAGES TO VERIFY CUSTOMER IDENTITY

Although Motor Vehicles uses finger images to investigate potentially fraudulent applications, it cannot use them to verify the identity of all customers applying for driver licenses or ID cards, the basic identification documents in California. Inadequate technology, questionable image quality, and privacy concerns from opponents of finger imaging prevent Motor Vehicles from using the images. The Legislature has yet to grant funds for an expensive technology upgrade requested by Motor Vehicles to make finger imaging an effective tool to cut down on driver license and ID card fraud. Yet for roughly two decades, state law has required Motor Vehicles to collect finger images from customers seeking original or renewal driver licenses or ID cards. The Legislature's declared intent in allowing Motor Vehicles to collect these images was to secure the accuracy and integrity of the identification system. Also, current users of

Users of computer-mapped finger-imaging systems say this is the most effective way of verifying an individual's identity.

finger-imaging systems, such as law enforcement, say this is the most effective way of verifying an individual's identity and is accurate between 98 percent and 100 percent of the time.

Inadequate Technology Hinders the Use of Computer-Mapped Finger Images

As early as the 1980s, federal law enforcement agencies began using the Automated Finger Identification System. This computerized system scans and digitizes a finger image by creating a map of the individual's unique ridge patterns and translating that map into a code that the computer can then search for and possibly match. Finger imaging is widely accepted by the public and by law enforcement communities as a reliable means of human recognition because it can answer, with a high degree of accuracy and speed, the questions: "Do I know who you are?" and "Are you who you claim to be?" The technology also eliminates any errors that human decision makers can cause.

Without the necessary technology, Motor Vehicles cannot ensure that a customer applying for a renewal or duplicate driver license or ID card is the true holder of the original document.

Although Motor Vehicles uses video capture stations to enter and store customers' photo, finger, and signature images in its database, the system is not as effective as it could be. Because it lacks the necessary technology, Motor Vehicles cannot ensure that a customer applying for a renewal or duplicate driver license or ID card is the true holder by conducting a one-to-one search, which would compare a finger image in its database against the image the customer is providing in person. Technology limitations further prevent Motor Vehicles from making sure that a new customer does not already hold a driver license or ID card under another name by using a one-to-many search, which would compare a new or existing finger image with all other images in the database. Motor Vehicles states that performing these searches requires hardware and software upgrades to its existing video capture stations at a cost of at least \$13.5 million. During fiscal year 2000–01, Motor Vehicles sought funding to begin these upgrades. However, the Legislature denied its request in May 2001 and as of August 2001 has not set aside any funds for upgrading the finger-imaging technology. Although the legislative record is unclear on why the request was denied according to the Legislative Analyst's Office *Analysis of the 2001–02 Budget Bill*, Motor Vehicles did not sufficiently develop its request, address employee oversight issues, or consider the potential impacts on privacy and efficiency.

Although the extent to which fraudulent driver licenses and ID cards play a role in identity theft is unknown, California citizens can suffer substantial financial losses from such theft. In 1997 the Legislature made it a public offense to willfully obtain personal identifying information, such as a driver license number, of another person without that person's authorization or to use that information to obtain, or attempt to obtain, credit, goods, or services in the name of another person without that person's consent. To further its support for cutting down on identity theft and other similar crimes, the Legislature should consider if it believes Motor Vehicles' use of finger images is a more effective way to verify an individual's identity.

The Quality of Images Taken So Far May Be Too Poor to Perform Searches

Unacceptable images can make one-to-one and one-to-many searches impossible and hinder Motor Vehicles' investigations. The finger images in Motor Vehicles' existing database date back to early 1990, but Motor Vehicles was not able to collect finger images that meet Federal Bureau of Investigation standards until 1999. Therefore, the finger images that Motor Vehicles has taken may not support computerized searches even if it does receive the funding to upgrade its technology. Since April 2000, a pilot study conducted by Motor Vehicles and the Department of Justice to test the reliability and usefulness of almost 1.3 million finger images taken by Motor Vehicles has been under way. However, after more than a year, Motor Vehicles has not had much success in obtaining any meaningful results concerning the overall quality of the finger images in its database. Therefore, Motor Vehicles may need to start over by collecting new images from every holder of a driver license or ID card.



Finger-imaging device

One challenge of finger imaging is the possibility of poor image quality caused by residue, such as dirt or body oils, on the finger as well as ridge patterns eroded by scrapes, years of heavy labor, or mutilation. Another challenge is that the quality of the finger image is highly dependent on the skill of the person capturing the image. When a customer applies for a new driver license or ID card, a field representative takes a finger image by having the customer place his or her finger on the video capture station and then pressing a button to record the image. The station's computer software evaluates the quality of the finger image and displays the image for the field representative to review. If the software considers the image acceptable but the field representative does not, the field representative can override the software and

capture another image. If the software considers the image unacceptable, the field representative cannot override the software and must try again to capture an acceptable image. However, after three unsuccessful attempts, the field representative can force the software to accept the image and record the last print taken, which may or may not be readable. Motor Vehicles told us that it plans to implement a pilot study at two of its field offices that will require a supervisor to approve the field representative's override after three unsuccessful attempts. It expects to complete this study by December 2001. This approval process is particularly important because even if Motor Vehicles obtains the funding to upgrade its technology, its current procedure of allowing field representatives to override the software after three unsuccessful attempts could contribute to the poor quality of images taken.

Privacy Rights Can Be Protected and May Not Outweigh the Benefits of Finger Imaging

The California Supreme Court found that finger imaging alone does not improperly infringe on an individual's right to privacy.

Some opponents of the use of finger imaging have raised both legal and policy concerns about the potential for this technology to interfere with individual privacy rights. However, with appropriate limitations on their use, finger images can be a legal and effective way to reduce identity fraud that can harm the public. The California Supreme Court, in *Persky vs. Department of Motor Vehicles*, addressed the specific issue of whether establishing a statewide identification system relating to driver licenses violates the right to privacy. In considering the issue, the court found that the Legislature adopted the fingerprint requirement to ensure the accuracy of Motor Vehicles driver license records and that deterring fraud promotes highway safety. The court also pointed to a long line of legal decisions finding that finger imaging alone does not improperly infringe on an individual's right to privacy. Similar reasoning would likely apply to the use of finger imaging for Motor Vehicles ID cards because the State has a legitimate interest in protecting the public from the use of these cards to facilitate identity theft or other similar crimes.

However, the California Supreme Court also found that the use of finger images is subject to the Information Practices Act, which places strict limits on the maintenance and dissemination of personal information. Therefore, if the Legislature decides to provide funding to upgrade Motor Vehicles' system, the Legislature should consider requiring Motor Vehicles to place limits on the use of finger images, particularly as technological advances increase the potential for using finger images to infringe on the

right to privacy. For example, recent scientific research suggests that finger imaging might disclose sensitive medical information about a person, such as certain illnesses or chromosomal disorders. To address both public and legal concerns regarding the use of finger images, Motor Vehicles must keep in mind the primary purpose for collecting the images and protect them against any unauthorized disclosures. If Motor Vehicles takes the necessary precautions against such disclosures, it should be allowed to use finger images to reduce fraud by more effectively verifying a customer's identity before issuing a driver license or ID card.

ITS RECENT REFORMS SHOULD REDUCE FRAUD, BUT MOTOR VEHICLES CANNOT MEASURE THE REFORMS' IMPACT

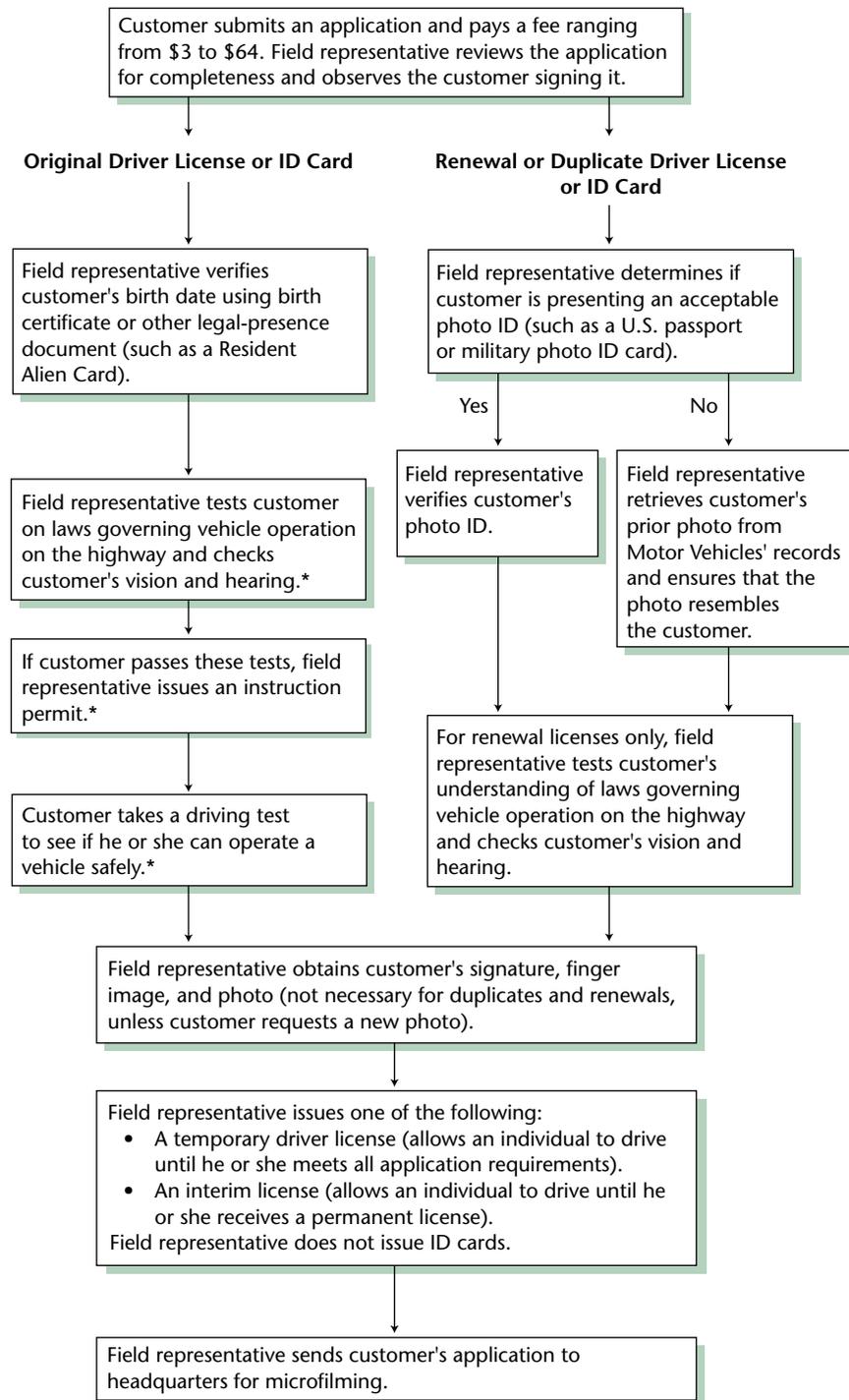
Last year a series of news articles reported the ease in obtaining fraudulent driver licenses, raising charges of lax processing and security procedures at Motor Vehicles. The articles asserted that Motor Vehicles issued thousands of fraudulent licenses to identity thieves, who use them to loot bank accounts and secure loans they never repay, and to illegal immigrants, who use them to establish legal status in California. Motor Vehicles immediately responded by implementing new reforms, such as electronically verifying Social Security numbers, retrieving customers' most recent photographs from its database, and requiring secondary verification of birth-date and legal-presence documents when issuing original licenses. Our review of 20 of the 170 field offices indicates that most employees are aware of Motor Vehicles' new fraud prevention procedures. However, Motor Vehicles is unable to measure the impact of its new reforms, so it cannot know how successful they have been in reducing identity fraud.

Current Process for Customers Applying for a Driver License or ID Card

The process of applying for a driver license or ID card has several steps, beginning with the customer submitting an application. A field representative then confirms the customer's identity by following one of Motor Vehicles' new fraud prevention procedures. Once the field representative completes the identity verification, the customer takes any applicable tests and then moves on to a finger-imaging and photographing station. Figure 1 provides an overview of the process.

FIGURE 1

Process for Applying for Driver Licenses and ID Cards



* This step does not pertain to customers applying for an ID card.

Electronic Verification of Social Security Numbers Improves the Integrity of the Motor Vehicles Database

On October 14, 2000, Motor Vehicles began electronically verifying with the federal Social Security Administration (SSA) the Social Security number, name, birth date, and gender on every driver license and ID card application. Electronic verification from SSA adds to the accuracy, reliability, and integrity of the Motor Vehicles database for driver licenses and ID cards. Rather than visually inspecting the Social Security card, the field representative requests an electronic confirmation of the data from SSA. This reform is also effective because Motor Vehicles will not issue a driver license or ID card without this verification.

To increase the accuracy of its driver license and ID card database, Motor Vehicles verifies information from applications with the federal Social Security Administration.

Motor Vehicles verifies the Social Security number, name, birth date, and gender of its customers by transmitting this information to SSA daily and receiving a response from SSA within 72 hours. The verification process has resulted in a mismatch rate of between 10 percent and 11 percent. Some of these mismatches—differences between a customer's name as it appears on Motor Vehicles and SSA records—occur because Motor Vehicles uses a person's true full name as it appears on birth certificates, marriage certificates, and other legal documents, while SSA is more flexible. A mismatch can also happen when a customer's Social Security number or birth date does not agree with Motor Vehicles and SSA records.

When a mismatch occurs, Motor Vehicles sends the customer a letter requesting additional information. Before May 2001, when a mismatch occurred relating to a name or birth date, the customer would have to correct either Motor Vehicles or SSA data before he or she could receive a driver license or ID card. According to Motor Vehicles data, on average, more than 3,500 people every day were receiving letters that Motor Vehicles was unable to verify data relating to their Social Security numbers. Each time a customer responded to Motor Vehicles' request for correct information, the information was resubmitted to SSA. This cycle could potentially continue for up to one year, because Motor Vehicles will not issue a driver license or ID card until it receives the correct information, and an application is valid for one year from the date Motor Vehicles receives the application fee.

As of May 2001 if SSA determines that a Social Security number, which initially shows as a mismatch, belongs to the customer shown on the Motor Vehicles database, it sends a certification letter directly to Motor Vehicles, eliminating the possibility of alterations or forgeries by the customer. This change also

eliminates the need for Motor Vehicles employees to resubmit data to SSA and reduces the customer's inconvenience of having to change his or her name with SSA if it does not match Motor Vehicles' record.

Photo Retrievals to Validate Customers' Identities Improve the Chances of Detecting Fraud

Another recent reform, begun on October 25, 2000, was Motor Vehicles requiring customers already in its database to validate their identity before being issued any temporary license, driver license, or ID card. Any customer applying for one of these documents must present acceptable photo identification, such as a California driver license or ID card, a U.S. passport, or a military photo ID card. If the customer does not present acceptable photo identification, the field representative retrieves the customer's prior photo from the video capture station and ensures that the photo resembles the customer before continuing the application process. However, if unable to confirm the customer's identity, the field representative flags the application for further review by the Driver License Fraud Analysis Unit (Fraud Analysis). The new photo retrieval process helps to strengthen Motor Vehicles' procedures because customers who cannot affirm their identities will not obtain the documents they are applying for. Motor Vehicles' Electronic Oversight Branch found that between October 2000 and June 2001, these new procedures reduced by 5 percent the number of duplicate licenses issued with new photos—the licenses most vulnerable to fraud.

Secondary Verification of Birth-Date and Legal-Presence Documents Should Reduce Fraud

Birth-Date and Legal-Presence Documents

Used to verify customers' birth dates and that their presence in the United States is legal.

Examples

- U.S. birth certificate
- U.S. passport
- Certificate of Naturalization
- Resident Alien Card
- Record of Arrival and Departure found on the back of an unexpired foreign passport.

Motor Vehicles' most recent reform began on January 2, 2001, when it implemented the requirement that field representatives obtain secondary verification, from specially trained employees, of all birth-date and legal-presence documents that customers submit with applications for original driver licenses and ID cards.

A field representative can no longer even start the process of issuing an original driver license or ID card if the customer does not have one of these required documents. First, the field representative must examine and verify the documents a customer

presents as proof of his or her true full name, birth date, and legal presence. Then the field representative writes his or her initials and the code for the document type on the application, indicating that he or she reviewed the documents for authenticity. As the customer waits, the field representative shows the customer's documents to a selected field office employee, trained in the detection of altered or fraudulent documents, for a secondary verification of all birth-date and legal-presence documents. If no specially trained employee is available, a manager or a field office investigator can be the secondary reviewer. The second examiner must also indicate approval of the documents by signing his or her first initial, last name, technician ID number, and date on the application.

If the customer's documents are unacceptable, the field representative holds the application and flags the transaction in the database as a potential fraudulent application. Then the field representative refers the customer to a local field investigator or photocopies the documents and sends them to Fraud Analysis for further review. Flagging the record prevents the customer from securing a fraudulent driver license or ID card at other Motor Vehicles offices using the same documents. If the customer returns to the office later with acceptable documents, he or she must speak with an investigator before proceeding with the application process.

Motor Vehicles Cannot Measure the Impact of Its New Reforms

Although the new reforms should reduce fraud, Motor Vehicles cannot measure their impact, partly because measuring deterrence is impossible. In other cases, Motor Vehicles simply lacks a tracking mechanism that would allow it to quantify the effect of a reform. Motor Vehicles recognizes that it is unable to track fraud trends and statistics and states that it is working on a way to establish trends and measure the effects of its procedures. However, until it can establish an effective measurement system, Motor Vehicles has no way of knowing how successful its reforms have been.

Electronically verifying Social Security numbers with SSA improves Motor Vehicles verification process; however, Motor Vehicles cannot quantify how effective this procedure is because it does not track information on how many customers with questionable Social Security information were not successful in obtaining fraudulent driver licenses or ID cards. According to Motor Vehicles,

on average, between 2 percent and 3 percent of requests it submits to SSA remain unresolved after 90 days. For example, using an average daily submission of 20,000 requests, potentially between 36,000 and 54,000 could be unresolved during each 90-day period. Motor Vehicles states that it does not investigate the causes of these unresolved requests and has no plans to do so.

Although the new photo retrieval procedure helps validate a customer's identity before the issuance of a temporary license, driver license, or ID card, the Field Investigations Branch does not know the number of fraudulent applications that this process has prevented.

Similarly, the new photo retrieval procedure helps Motor Vehicles validate a customer's identity before issuing a temporary license, driver license, or ID card—but the procedure's effect on reducing fraud is unclear. Between October 25, 2000, and August 31, 2001, field representatives used this new procedure to flag more than 3,600 records as potential fraudulent applications. Fraud Analysis receives these flagged records, analyzes the history of photos, and forwards suspected fraudulent applications to the Field Investigations Branch (Field Investigations). For these 3,600 records, Fraud Analysis believes that nearly 1,600 of the customers appearing before the field representative did not resemble the photos in Motor Vehicles' database. For another more than 1,100 records it believes that a fraudulent driver license or ID card may have been issued since the customer resembled prior photos but not the most recent in the database. Further, because about 190 customers simply left the field office when the field representatives told them that their photos would be retrieved, Fraud Analysis could not draw any conclusions. However, Motor Vehicles cannot determine the number of actual fraudulent applications that are ultimately confirmed because Field Investigations pools everything it receives from Fraud Analysis with its existing caseload and does not identify the number of suspected fraudulent applications resulting only from the photo retrieval process.

Motor Vehicles also cannot quantify the effect that its new secondary verification procedure for all customer birth-date and legal-presence documents has had on reducing fraud. Because this new procedure prohibits a customer from starting a transaction without presenting birth-date and legal-presence documents, it is hard to determine how many customers with potentially fraudulent documents have been deterred. Also, Motor Vehicles changed its procedure for reviewing applications that field representatives flag for further review. Formerly, field representatives would send photocopies of potentially fraudulent birth-date and legal-presence documents to Fraud Analysis. Now they can refer the customer to a local field investigator or send photocopies to Fraud Analysis for further review. Because Fraud Analysis tracks the number of cases it receives relating to potentially

fraudulent birth-date and legal-presence documents, in fiscal year 2000–01 we were able to identify a decline of about 60 percent in the number of cases Fraud Analysis has received since the procedure began. However, Motor Vehicles’ field investigators do not track the number of cases they receive relating to this procedure, so Motor Vehicles is unable to determine the full effect of this reform. Specifically, prior to this procedure, field representatives could flag an application if the customer’s documents were unacceptable. Therefore, Motor Vehicles has no way of knowing if the apparent increases in fraudulent applications are based solely on the second employee’s verification of documents.

DESPITE PROMISING REFORMS, MORE IMPROVEMENTS ARE NEEDED TO REDUCE FRAUD

Although Motor Vehicles has taken significant action to reduce the possibility of issuing fraudulent driver licenses and ID cards, some reforms could be expanded. For example, photo retrieval to identify a prior customer would be a stronger reform if a second employee confirmed the original field representative’s verification that the customer matched the retrieved photograph. Also, our review of the processes for issuing driver licenses and ID cards revealed additional opportunities for Motor Vehicles to improve its controls to reduce fraud. A new method Motor Vehicles is working on to electronically verify that each computer request for a driver license or ID card has a paper application to back it up will not work unless field managers can ensure that employees enter application bar-code numbers into the system. Further, Motor Vehicles has not taken steps to evaluate and implement many of the Anti-Fraud Task Force (task force) recommendations on ways to reduce driver license and ID card fraud.

A further improvement to Motor Vehicles’ fraud prevention system would be to require two employees to validate photo retrievals when issuing a temporary license, driver license, or ID card to existing customers.

Motor Vehicles Could Improve Its Photo Validation Reform

As previously discussed, Motor Vehicles began requiring an existing customer to validate his or her identity before obtaining a temporary license, driver license, or ID card. When a customer lacks an acceptable photo ID, a field representative retrieves the customer’s prior photograph to verify physical resemblance. However, Motor Vehicles would better guard against fraud if it required two employees to validate photo retrievals when issuing these documents. Without this accountability—similar to the secondary verification procedures that exist for reviewing birth-date and legal-presence documents when issuing an

original driver license or ID card—there is still some risk that an employee could assist a customer in assuming the identity of another individual.

Motor Vehicles believes that this risk is minimal because there is no evidence of employees helping customers assume identities through fraudulent photo verification. Although Motor Vehicles does not have any data to support this position, it will consider having Fraud Analysis select a sample of new photos of customers requesting duplicate or renewal driver licenses and compare them with prior photos to determine whether it is the same person. The results of these comparisons would enable Motor Vehicles to measure the extent of fraud in this area and determine if secondary photo comparisons by Fraud Analysis would be beneficial for all duplicate or renewal driver license and ID card requests involving new photos.

To Reconcile Paper Applications With Corresponding Computer Entries, Employees Must Enter Bar-Code Numbers for All Applications Received

Motor Vehicles' Electronic Oversight Branch is working on an electronic reconciling procedure that will allow it to know whether a field office employee sends all completed driver license and ID card applications to headquarters for microfilming, a process that assists Motor Vehicles in the prosecution of customers who make false statements on their applications. The electronic reconciling procedure would ensure that each computer request for a driver license or ID card has a corresponding paper application. For the procedure to be manageable, field representatives must first comply with existing procedures that require them to enter into a database a bar-code number for every application. Without the bar-code numbers to electronically track the microfilm location of the application, Motor Vehicles has to manually search for applications that are missing bar-code numbers.

Motor Vehicles found that between January and March 2001, bar-code numbers had not been entered for more than 112,000 (14 percent) of the roughly 802,000 applications it processed. Although the Electronic Oversight Branch's implementation of its reconciling procedure may not be complete until December 2001, Motor Vehicles needs to ensure that field representatives enter bar-code numbers for all paper applications and then send the applications to headquarters for microfilming. Because employees are not consistently following these steps, until the new procedure is in effect, Motor Vehicles' ability to ensure the

The absence of bar-code numbers to electronically track the microfilm location of customer applications hampers Motor Vehicles' ability to ensure the prosecution of customers who falsely obtain driver licenses or ID cards.

prosecution of customers who falsely obtain driver licenses or ID cards is hampered. Presently, Motor Vehicles does not know if field representatives send all completed driver license or ID card applications to headquarters for microfilming.

Motor Vehicles Needs to Address the Remaining Anti-Fraud Task Force Recommendations

With recent reforms, Motor Vehicles has fully implemented 8 of the 55 recommendations of its task force but has yet to even evaluate most of the remaining 47 task force recommendations related to driver license, ID card, and employee fraud. Motor Vehicles is thus delaying the implementation of some recommendations that may be beneficial and feasible.

In November 2000 Motor Vehicles assembled the task force, which includes Motor Vehicles' staff as well as representatives from law enforcement, financial institutions, the insurance industry, and privacy rights groups, to provide feedback on all issues dealing with fraud at Motor Vehicles. Motor Vehicles reports that it has completed implementing 8 of the 55 recommendations by taking the following actions:

- Revised its mission statement and policy on identity fraud or theft.
- Created a consumer fraud hotline and Web site.
- Established its new photo retrieval and secondary verification procedures.
- Established a single point of contact for reporting fraud and identity theft.
- Added additional security features on the current driver license.

Several of the task force's pending recommendations also address issues identified during our audit, such as the inability to track fraud trends and statistics to establish the extent of fraud and the ability of Motor Vehicles' field representatives to override rejection of finger images after three attempts.

In one pending recommendation, the task force suggests that Motor Vehicles improve its background screening of new employees. To accomplish this goal, according to the task force, Motor Vehicles should establish a database to monitor which

employees have had background checks, process all job applicants' finger images through the Federal Bureau of Investigation's national database, and require potential employees to submit their finger images before being hired. Currently, Motor Vehicles' policy is to perform background checks on all employees in its field offices and headquarters working in positions of trust, which includes positions that handle confidential and sensitive records. To address the task force recommendation, Motor Vehicles began using a database on September 4, 2001, to monitor all employees' background checks. It also submitted a proposal to the State Personnel Board and a union requesting that all applicants be subjected to background checks. This proposal has reached an impasse with the union. However, the SPB conditionally approved its proposal in August 2001, and Motor Vehicles expects to implement the proposal by January 2002. Finally, effective April 2001, Motor Vehicles has given supervisors the option to delay hiring offers until they receive the results of background checks for individuals applying for positions of trust, but supervisors already have the option of terminating employees whose background checks are received after hiring and are unacceptable.

Several of the remaining 47 initiatives are beyond Motor Vehicles' control, and many, such as a recommendation to clarify state law regarding which county has jurisdiction for prosecution, would require legislation to implement. Motor Vehicles may determine that certain other recommendations are not beneficial or feasible. Because it did not require responsible divisions to submit responses until mid-September and October 2001 for some of the recommendations and has not established response due dates for others, Motor Vehicles is unable to give a timely evaluation of the merits of these recommendations. However, Motor Vehicles told us it has taken action on other fraud-related issues that the task force did not specifically address such as providing letters to its customers acknowledging that they were a victim of identity theft so that they can use this information to notify their banks, credit card companies, or other interested entities.

Because it did not require responsible divisions to submit prompt responses for some of the task force's recommendations, Motor Vehicles is unable to give a timely evaluation of the merits of these recommendations.

New Procedures Increase Waiting Times, but Motor Vehicles Has Taken Steps to Mitigate This Effect

Although Motor Vehicles' new fraud prevention procedures help protect its customers' identities, the reforms have also increased customer waiting times at the field offices. Since Motor Vehicles implemented the new procedures, according to its data, field office waiting times have extended an average of 1.5 minutes for

As a result of Motor Vehicles' recent reforms, field office waiting times have gone up on average by 1.5 minutes for customers with appointments and 9.3 minutes for customers without appointments.

customers with appointments and 9.3 minutes for customers without appointments. Motor Vehicles has acted to mitigate these extensions. For example, this past January, Motor Vehicles launched online appointment scheduling, which has increased overall scheduling roughly 20 percent from last year. In addition, Motor Vehicles has been steadily expanding its electronic traffic management system (queuing system), which now operates in 26 field offices. Piloted in 1998, the queuing system has cut down on customers' long waits in line. Both the queuing system and online scheduling innovations have significantly improved customer perceptions of Motor Vehicles.

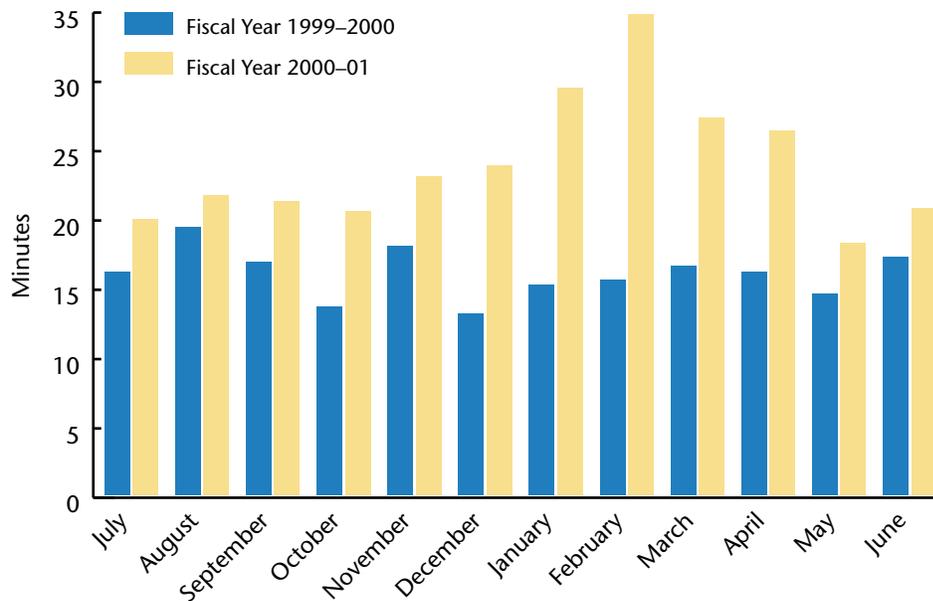
As Figure 2 shows, since reforms began in October 2000, field office waiting times for customers without appointments steadily increased through February 2001. The Motor Vehicles' field offices in Region 6, which covers the majority of Los Angeles County, were showing an average increase of 45 minutes per customer from the previous year. Since March 2001, waiting times have begun to decrease; however, they are still higher than the previous year. According to Motor Vehicles, the apparent decrease in waiting times in April and May are not indicative enough in themselves to identify a trend, especially since driver license volumes traditionally decrease during these months and begin to increase again in June. However, Motor Vehicles believes that its implementation of online appointment scheduling and a queuing system may have helped to reduce waiting times during this period.

Responding to customer needs, on January 8, 2001, Motor Vehicles implemented an online appointment system that enables customers to schedule appointments using a personal computer and thus reduces their waiting times. In the first month of operation, overall driver license appointment scheduling increased nearly 30 percent from the previous year. Between January and July 2001, the average increase in driver license appointments was nearly 20 percent. Also, results of a Motor Vehicles' survey show that nearly 20 percent of the customers who used the online system had not previously scheduled appointments before visiting field offices.

Motor Vehicles' electronic traffic management system, piloted in 1998, also helps mitigate waiting time increases. For example, using this queuing system, field office managers can identify the longest waiting time for current customers, the number of customers waiting for each service, and the employees currently available to serve them. This data helps management reallocate

FIGURE 2

Waiting Times for Customers Without Appointments



Source: Motor Vehicles' Field Operations Division.

Note: New procedures were implemented beginning on October 14, 2000.

staff throughout the day to prevent long waiting times. As of June 2001, 26 of Motor Vehicles' larger, busier field offices were equipped with the system. Motor Vehicles plans to install systems in 66 additional crowded field offices and in its 8 regional offices by the end of fiscal year 2002-03. The average initial cost per office to install a queuing system is roughly \$55,000.

The queuing system has had a significant effect on customer perceptions of Motor Vehicles. Customers of offices that piloted the system perceived that they were served faster after the installation of the system. Also, results of our interviews with field office managers and customers indicate that the queuing system improves customer service and reduces the stress levels of both customers and employees. Motor Vehicles also plans to post real-time data from the queuing systems, such as current waiting times by office, to its Web site and at field offices so that customers can better choose when and where they wish to conduct business. Motor Vehicles believes that this capability will further improve customers' attitudes towards waiting times.

Customers believe that Motor Vehicles' use of electronic traffic management systems in its larger, busier field offices improves customer service and reduces their stress levels.

Finally, in April 2001, Motor Vehicles installed 35, or about 14 percent, more video capture stations in its largest field offices to lessen customer waiting times resulting from heightened photo retrieval activity. However, some employees interviewed during our field office visits told us that Motor Vehicles needs to provide more video capture stations. For example, there were 110,052 field office photo retrievals in June 2001, an increase of 44 percent from June 2000. This increase, along with the employee interviews, indicates that there may be a need for even more stations and possibly additional staffing.

In October 2000 Motor Vehicles prepared an analysis of its staffing needs pertaining to the new photo retrieval procedure and received approval for 21 additional positions to operate the 35 new video capture stations. However, according to its budget advisor, Motor Vehicles has yet to complete a similar analysis to assess the impact of the other new fraud prevention procedures on its staffing levels. Until Motor Vehicles completes such an analysis, it does not know if it has sufficient staff to effectively carry out its new procedures.

MOTOR VEHICLES' FRAUD DETECTION TRAINING NEEDS IMPROVEMENT

Motor Vehicles is not maximizing the benefits of its training course in detecting fraudulent documents. The Field Operations Division (Field Operations) and field office managers' goals conflict regarding which employees should receive the training. Also, database flaws prevent Field Operations from knowing if it even meets its goals. Further, in interviewing trainees and reviewing departmental evaluations, we found significant concerns with the trainers, the curriculum, and available resources. Problems include a lack of hands-on experience with original documents, uniformity among trainers' presentations, and time to cover the material. The Investigations and Audits Division (Investigations) points to a lack of funds to develop the trainers' skills and to purchase needed materials. Meanwhile, inconsistent classes and other problems make the training less useful to employees responsible for fraud detection and prevention and a less effective tool for Motor Vehicles in its efforts to reduce the issuance of fraudulent driver licenses and ID cards.

Some Motor Vehicles Field Offices Are Not Adhering to the Training Goals Set by the Field Operations Division

Field Operations established certain short- and long-term goals regarding the provision of fraud training to field office employees. However, our interviews with a few field office managers reveal that their goals contradict those of Field Operations' management. In addition, Field Operations' management was unaware of the inconsistency of its goals with those of the field office managers until we brought it to their attention because flaws in the training databases prevent it from effectively monitoring compliance. Without good data and agreement between levels of management, Field Operations cannot guarantee it meets its goals of ensuring that field office employees are knowledgeable of fraudulent document detection procedures.

In 1999 Investigations developed a fraudulent document detection lesson plan, for use within Motor Vehicles as well as for outside entities such as law enforcement agencies and insurance companies. The lesson plan addresses fraud relating to driver licenses and ID cards, identity theft, birth certificates, Social Security cards, Immigration and Naturalization (INS) documents, passports, and military photo ID cards. However, Investigations did not begin to discuss the need for providing this training to field office employees involved with issuing driver licenses until October 2000, when a series of news articles reported the ease in obtaining fraudulent driver licenses. Motor Vehicles gave Investigations the responsibility to teach this course to field representatives beginning on November 14, 2000. Investigations taught 20 classes in the first 30 days.

Motor Vehicles' Field Operations Branch incorrectly thought that it met its initial goal of training at least two employees from each of the 170 field offices on how to detect fraudulent documents.

Field Operations had an initial goal of training at least two employees from each of the 170 field offices by December 31, 2000, just before Motor Vehicles' new secondary verification of birth-date and legal-presence documents was to begin in January 2001. Field Operations' long-range goal is to train all field office employees involved with issuing driver licenses and ID cards. However, in 3 of the 20 field offices we visited, office managers, who recommend which employees in their field office will receive fraudulent document detection training, told us they do not believe all employees should receive this training. Lack of consensus between Field Operations' management and field office managers makes it difficult for Field Operations to meet long-term goals.

Investigations reports that, as of December 31, 2000, 369 employees received training, which illustrates that it was possible to train 2 employees from each field office (a total of 340 employees) within that short period. However, Field Operations incorrectly thought that it met its initial goal. Because Investigations' database only reports the training date, instructor, location, and total number of attendees, Field Operations had not analyzed the 369 employees to identify how many were actually headquarters employees, not field office employees. Additionally, Investigations' database contains errors because classes were omitted or entered twice. The Departmental Training Branch of Motor Vehicles' Administrative Services Division has an employee training database that is also available to Field Operations for monitoring compliance. This database does record the necessary information to identify the employee's field office location. However, it also contains errors—some employees who took the training are not shown. Moreover, the database does not have the capability to perform various sorts to summarize information by field office or headquarters locations. Therefore, Field Operations is unable to use data from Investigations or the Departmental Training Branch to monitor whether its training goals are being met.

Both of Motor Vehicles' databases for tracking employee training information contain errors.

Our analysis of those employees who attended classes as of December 31, 2000, using data from the Departmental Training Branch's database, reveals that 49 field offices sent only one employee for training and 10 field offices sent none of their employees. This would mean that 35 percent of the 170 field offices did not meet Field Operations' initial goal. Additionally, review of Departmental Training Branch's database as of June 30, 2001, shows that 11 field offices still have sent only one employee for training and one field office has yet to send anyone. Two of the 11 field offices have only one employee.

Field Operations originally planned for all field representatives to receive fraud detection training, with the intent that they be able to detect obvious fraudulent or counterfeit documents but not become document experts. It feels that the current training course is sufficient for attendance by all field representatives, as part of ongoing driver license training. Field Operations agrees that it needs to address and correct the database issues to adequately assess that it is meeting its goals.

Training Is Inconsistent and May Not Meet Staff Needs

Our employee interviews and review of training class evaluations indicate that the current fraudulent document detection training course needs considerable revision. Rather than providing adequate hands-on experience with original documents, the course primarily uses photocopies, and trainers are inconsistent with each other in what they present and how they present it. Investigations is working on some of the weaknesses; however, additional changes—estimated by Investigations to cost roughly \$135,000—are necessary to ensure the training benefits field office employees.

Employees we interviewed during our site visits told us about improvements that would make the fraudulent document detection training more useful to them. For example, employees said that the training should include a more thorough review of birth certificates, including those from out of state, and should use original documents rather than photocopies. Employees also felt that trainers should use more examples to illustrate differences between authentic and fraudulent birth-date and legal-presence documents. A few employees indicated that investigators teaching the course needed to be more qualified and better prepared. For example, one employee said that the investigator who taught the class was not knowledgeable about all of the documents and was not prepared to discuss areas outside of his or her specialty. Finally, many employees said that the 8-hour class was not long enough to cover the material adequately.

Investigations is aware of the shortcomings of the training. Staff in its program support unit completed evaluations after observing the trainers during a quality assurance pilot conducted in May and June 2001. The evaluators said that a main area needing improvement is the lack of uniformity and standardization among trainers presenting the course. For example, not all trainers use the handouts, videos, and PowerPoint presentations that the curriculum requires. Trainers also did not adhere to the times specified for each topic. The evaluators also indicated that trainers blame lack of resources, such as real passports and detailed handouts to provide attendees, for their inability to thoroughly address issues relating to passports, INS documents, and military photo ID cards.

Trainees evaluating the fraudulent document detection training course suggested that it needs to more fully address the identification of authentic and counterfeit documents.

Staff in the program support unit of Investigations also analyzed the comments trainees made on their evaluation forms after attending the course between November 2000 and June 2001. Paralleling comments from our site visits, trainees suggested providing more authentic and counterfeit documents for review, extending the class to two days, giving each employee a desk reference manual on fraud detection, and having guest speakers from INS and SSA.

In September 2001 Investigations conducted a one-day meeting with trainers and support staff to emphasize the need for consistent training and to begin developing a uniform lesson plan using input from trainers, employee evaluations, and Field Operations management. Investigations states that most of the problems have resulted from a lack of funding to purchase critical tools and to develop trainers' skills and abilities. Another source of problems is that Investigations has been without a deputy director since January 2001 and without a chief for its field investigative staff for even longer. Although it has numerous short-, mid-, and long-term plans, including improving the skills of the trainers and purchasing equipment, Investigations says it lacks the funding, roughly \$135,000, to accomplish these goals.

RECOMMENDATIONS

If recent reforms prove insufficient, the Legislature should reconsider funding to support Motor Vehicles' upgrade of its finger-imaging technology. If it chooses to fund the upgrade, the Legislature should consider protecting against unauthorized dissemination of finger images by limiting access to Motor Vehicles' imaging data to only those entities the Legislature finds have a legitimate interest in protecting the public, such as state and local law enforcement agencies. The Legislature should also consider imposing criminal sanctions for the unauthorized use of the data.

Additionally, if the Legislature approves the use of finger imaging, it might want to require Motor Vehicles to establish controls that protect the privacy of California citizens. More specifically, the Legislature should consider directing Motor Vehicles to create procedures for the following activities:

- Establishing controls to prevent the improper disclosure of finger images.

- Storing physical documents that support the data in a secure area.
- Using sufficient firewalls and other electronic security measures to secure the computer network from “hackers” and criminal interests.
- Limiting access to the database and setting up an “audit trail” to identify users of the data.

To further improve its existing controls and reduce waiting times for customers at field offices, Motor Vehicles should take the following steps:

- Train field representatives to capture good-quality finger images and prohibit them from bypassing system requirements for obtaining readable customer images without prior approval from their managers.
- Establish mechanisms to measure the effectiveness of its recent and future reforms.
- Continue to work on the plan to electronically reconcile system transactions against applications sent for microfilming at headquarters to ensure that an application supports each transaction. Further, field office managers should make sure that field representatives enter bar-code numbers for all paper applications before sending the applications to headquarters.
- Instruct Fraud Analysis to conduct a study to determine the benefits of verifying identification by comparing new photos of existing customers obtaining temporary licenses, driver licenses, or ID cards with photos already in the Motor Vehicles database.
- Establish deadlines for staff to address all of the task force recommendations and conduct a timely evaluation of the merits of each recommendation.
- Continue its efforts to decrease field office waiting times by installing additional queuing systems and posting real-time data to its Web site. Also, determine if it needs to install more video capture stations for photo retrieval in the field offices. Finally, it should complete a staffing analysis to assess the impact that the recent reforms have had on its ability to carry out its procedures.

- Instruct Field Operations management to meet with field office managers to reiterate training expectations and monitor them for compliance with Field Operations' training goals.
- Correct training database errors and modify the Departmental Training Branch's database to allow users to view and sort employees' attendance at the training course for fraudulent document detection by reporting unit location.
- Continue to communicate with trainers and supervisors regarding Motor Vehicles' commitment to standardization and uniformity. Determine if Investigations needs additional funding to implement short-, mid-, and long-term goals for improving its training program. ■

CHAPTER 2

The Investigations and Audits Division Needs Better Policies, Procedures, and More Staff to Effectively Resolve Fraud Complaints

CHAPTER SUMMARY

Despite its safeguards against driver license and identification card (ID card) fraud, the Department of Motor Vehicles (Motor Vehicles) finds that both customers and employees sometimes violate procedures and break the law. Motor Vehicles' Investigations and Audits Division (Investigations) is responsible for looking into cases of possible fraud. However, a lack of procedures and resources hinder Investigations' inquiries into driver license and ID card fraud. Without improvements, Investigations will remain limited in how well it can carry out its mission of stopping fraud, assisting victims, and helping to prosecute wrongdoers. For example, the Field Investigations Branch (Field Investigations) lacks procedures dictating how its staff should manage and resolve complaints. Consequently, staff use varying methods to record a complaint's open and close dates in Field Investigations' case management database. Additionally, Field Investigations does not account for any time that cases may have sat in other units such as Investigations' Driver License Fraud Analysis Unit (Fraud Analysis). Motor Vehicles is thus unable to accurately determine how long its cases remain open and justify what its true staffing needs are.

A weakness in Field Investigations' case management database also prevents its investigators from sharing information such as fraud trends between offices. Additionally, Fraud Analysis lacks sufficient staffing to handle an increased workload caused by Motor Vehicles' new fraud prevention procedures and consumer fraud hotline. Finally, Motor Vehicles has not established a clear policy that precisely identifies the role of the Special Investigations Branch (Special Investigations) in investigating employee misconduct and therefore cannot ensure that it investigates all questionable employee activities or that employees participating in these activities receive consistent discipline.

BACKGROUND

Investigations has the following branches and unit that assist in detecting and preventing customer and employee fraud relating to issuing driver licenses and ID cards:

- Field Investigations has staff located throughout California in 30 offices overseen by eight area commanders. Field investigators are responsible for investigating criminal activity taking place in and around field offices, parking lots, and surrounding property and informing field office employees, managers, and regional administrators of this activity.
- Special Investigations is responsible for investigating all allegations of employee misconduct. Field Investigations' area commanders are to report to Special Investigations all known incidents of actual or suspected theft of state property and embezzlement or fraud occurring within Motor Vehicles.
- Electronic Oversight Branch develops and uses automated techniques to monitor for fraudulent and unauthorized transactions initiated by Motor Vehicles employees, customers, and other individuals who update, purchase, or distribute Motor Vehicles data online.
- Fraud Analysis provides technical assistance such as analyzing computer-mapped finger images (finger images) and photos to Motor Vehicles field investigators and staff within other divisions, law enforcement agencies, and other state agencies.

MISSING PROCEDURES AND FLAWED DATA PREVENT MOTOR VEHICLES FROM PROPERLY MANAGING ITS COMPLAINTS

Working in 30 offices around the State, Field Investigations staff have no procedures specifying how they should manage and resolve complaints. Consequently, staff use different methods to record a complaint's open and close dates in Field Investigations' case management database. Additionally, although many cases originate in other units such as Fraud Analysis, Field Investigations

does not account for time cases sat in these other units. As a result, Motor Vehicles is unable to accurately determine how long its cases remain open. For example, in our review of a sample of Field Investigations' case files, we found one case that took 441 days to close, yet it was shown in Field Investigations' database as being open for only 61 days. However, Field Investigations did not receive this case until it was already 378 days old. Fraud Analysis believes that it needs additional staff to prevent delays in referring cases like this to Field Investigations and to manage a 12-month backlog in its workload. Case management also suffers from a weakness in Field Investigations' database that prevents investigators from sharing information such as fraud trends between offices. Because of the lack of formal case management procedures, flawed data, and an inadequate database, Motor Vehicles cannot properly manage its complaints or evaluate its staffing needs.

Field Investigations Lacks Procedures Specifying How Its Staff Should Manage and Resolve Complaints

Generally, regulatory entities that protect public safety have a clear process for managing and resolving complaints. One would expect Field Investigations to have procedures that instruct its investigators, at a minimum, on how to log in complaints when they come in, when to send acknowledgment letters to complainants, how to prioritize and assign complaints, and when to complete an investigation and report results. However, Field Investigations lacks case management procedures for its investigators, who are left on their own to decide such things as when to open, close, or report on an investigation.

Because Motor Vehicles' Field Investigations Branch lacks written procedures on how to manage complaints, investigators are left on their own to decide such things as when to open, close, or report on an investigation.

Field Investigations receives complaints from customers, law enforcement agencies, and other Motor Vehicles units and employees. Field investigators also initiate complaints resulting from their own activities, such as reviewing suspected fraudulent or counterfeit documents that customers present to the field representatives. Table 3 on the following page shows the number of complaints relating to potentially fraudulent driver licenses and ID cards that Field Investigations opened and closed during the past five fiscal years.

TABLE 3**Complaints Opened and Closed
From Fiscal Years 1996–97 Through 2000–01**

	1996–97	1997–98	1998–99	1999–2000	2000–01
Complaints opened	6,580	7,584	6,718	7,705	7,955
Complaints closed	5,895	6,627	7,215	7,538	8,190

Source: Motor Vehicles' Investigations and Audits Division.

The lack of written procedures for managing complaints prevents Motor Vehicles from accurately determining how long it takes to conduct an investigation from start to finish. Field Investigations staff are inconsistent about what dates they use to record cases as opened and closed. For example, staff may record a complaint's open date as the date Field Investigations receives the case, the date the supervisor approves it to be opened, or the date it is input into the system. The open date also does not reflect time the case may have been with another unit, such as Fraud Analysis. Likewise, staff may record a complaint's close date as the date they complete work on the case or the date the supervisor reviews it.

Motor Vehicles states it did not establish procedures dictating how field investigators should manage complaints, thinking it more appropriate for area commanders to establish their own procedures. However, when we questioned area commanders, we found that only one had established formal procedures.

Besides clear procedures, field investigators need the ability to share case information among offices. However, Field Investigations' case management database prevents such sharing of information. Sharing data among offices would enable field investigators to track current fraud trends, view similar cases, and search for cases involving the same subject. After we brought this weakness to the acting deputy director's attention, he submitted a letter to the director proposing that Motor Vehicles immediately start the development of an improved case management database. Motor Vehicles is also considering the development of a database that will allow Investigations to track

information on fraudulent driver license and ID card use as well as victims and suspects of identity theft so that it can provide better statistical data.

In our review of the case files of 16 complaints that were closed between June 1, 2000, and June 20, 2001, we found several complaints that were open substantially longer than what was shown in Field Investigations' database. Table 4 shows the 7 complaints in our sample that were open the longest.

TABLE 4

Seven Complaints From Our Sample With the Largest Disparity in the Number of Days Cases Were Open June 1, 2000, Through June 20, 2001

Case	The Number of Days the Case Was Open According to the Discovery Date in Motor Vehicles' Case Files	The Number of Days the Case Was Open According to Motor Vehicles' Case Management Database	Difference
1	599	278	321
2	549	29	520
3	447	267	180
4	441	61	380
5	396	24	372
6	266	90	176
7	265	7	258

Field Investigations reports that the 8,190 complaints it closed in fiscal year 2000–01 were open an average of 71 days. We question this figure because for 16 complaints we reviewed, we found that average days open according to the discovery date found in the case files was 221 days, compared with 68 days indicated by Field Investigations' database. Eight of the 16 cases were referred from Fraud Analysis, 6 of which were already an average of 174 days old when Field Investigations received them. Because we were unable to determine the date that Fraud Analysis referred the other 2 cases to Field Investigations, we do not know how old those cases were when Field Investigations received them.

Field Investigations also reports that it has roughly 1,200 complaints outstanding as of June 30, 2001, but we question this figure because not all cases outstanding are logged into its database. Nevertheless, to address its outstanding complaints, Motor Vehicles requested 12 additional investigators for fiscal year 2001–02. However, the Legislature denied its request. Consequently, Motor Vehicles contends that because Field Investigations is insufficiently staffed, cases sit for long periods before it opens them.

New Fraud Detection Procedures Have Significantly Increased the Fraud Analysis Unit’s Workload

As discussed earlier, we reviewed 16 investigations and found that Motor Vehicles took an average of 221 days to close each case. An increase in Fraud Analysis’ workload and insufficient staff have contributed to Motor Vehicles inability to resolve cases in a timely manner. Responding to requests from various departmental and external sources, Fraud Analysis technicians detect potential fraud by analyzing customers’ finger images, photos, and handwriting, as well as various documents such as birth certificates. Then they prepare cases and send them to either Field Investigations or other appropriate Motor Vehicles divisions for administrative or criminal action.

At the end of fiscal year 2000–01, Fraud Analysis had a backlog of cases that was more than triple that of the previous fiscal year, partly because of Motor Vehicles’ new consumer fraud hotline and new fraud prevention procedures, which resulted in 6,300 cases for Fraud Analysis technicians to handle. Fraud Analysis states that it needs additional technicians to manage the rising caseload. Unless they are able to keep up with the new cases, Fraud Analysis technicians cannot effectively help Motor Vehicles and law enforcement agencies detect and prosecute criminal fraud. Table 5 shows the growing imbalance between the number of open cases and staff to handle them.

TABLE 5**Fraud Analysis Unit's Caseload and Staffing**

	1998-99	1999-2000	2000-01
Cases received	13,182	27,481	22,175
Cases on hand at June 30	N/A*	1,831	6,592
Authorized positions	21	19	23

Source: Motor Vehicles' Investigations and Audits Division.

* Motor Vehicles was unable to provide data for cases on hand in fiscal year 1998-99.

As Table 5 illustrates, Fraud Analysis staffing has not kept up with the dramatic increase in cases. In fiscal year 2000-01, two significant changes increased Fraud Analysis' workload. First, as previously discussed, in October 2000 and January 2001, respectively, Motor Vehicles implemented new procedures requiring Field Operations staff to retrieve the most recent photo in the Motor Vehicles database to verify the identity of its renewal and duplicate customers and to perform secondary verification of customer birth-date and legal-presence documents. If the photo in the database does not match the customer, Motor Vehicles field representatives forward the information to Fraud Analysis for investigation. If the customer's documents are unacceptable, field representatives may forward copies to local field investigators or Fraud Analysis. Between October 25, 2000, and June 30, 2001, Fraud Analysis received about 4,400 of these types of referrals. Second, in April 2001, Motor Vehicles established a consumer fraud hotline to allow customers to report suspected identity theft. Assigned to handle the calls, Fraud Analysis received almost 1,900 referrals from the hotline between April 2001 and June 2001.

In fiscal year 2000-01, investigative support staff, which includes Fraud Analysis, worked roughly 5,100 hours in overtime. Despite this extra effort, Fraud Analysis still had roughly 6,600 cases on hand at the end of the fiscal year. Although Fraud Analysis received six temporary positions in March and April 2001, it believes these positions should be permanent and that at least another 24 more technicians are necessary to manage its

workload. For example, Fraud Analysis told us that it received an additional 3,700 referrals from the hotline in the first two months of fiscal year 2001–02. However, Fraud Analysis has yet to complete a comprehensive staffing analysis that addresses its need relating to processing cases, handling calls to the consumer fraud hotline, and training new staff.

CLEARER POLICIES AND DEFINITIONS ARE NEEDED TO ENSURE THAT SPECIAL INVESTIGATIONS RECEIVES ALL EMPLOYEE FRAUD CASES

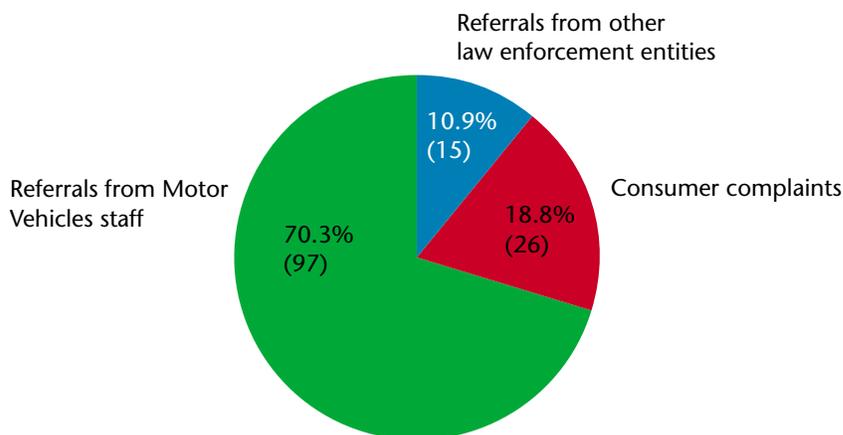
Investigations' policy and procedure manual defines Special Investigations' primary responsibility as investigating all allegations of employee misconduct. However, this definition is inconsistent with Motor Vehicles' Zero Tolerance Policy on Employee Fraud or Dishonesty, which allows its employees to report possible fraudulent or dishonest employee activities to a supervisor or directly to Special Investigations. Moreover, clear definitions of employee misconduct and fraudulent or dishonest behavior do not exist, creating inconsistencies in staff reports of possible fraudulent activity. Finally, Special Investigations does not receive all allegations of questionable employee activities because Motor Vehicles lacks procedures on how managers are to report employee misconduct and fraudulent or dishonest behavior. For example, most regional administrators require their staff to submit to them, not to Special Investigations, reports of potential employee fraud. Until it clearly establishes definitions and policies, and identifies Special Investigations' role in investigating employee misconduct, Motor Vehicles cannot ensure that it investigates all questionable employee activities or that employees participating in these activities receive consistent discipline.

Special Investigations receives complaints from customers, outside law enforcement agencies, and numerous sources within Motor Vehicles. Figure 3 shows the percentage of complaints received from each source during fiscal year 2000–01.

Motor Vehicles' Special Investigations Branch has an unclear mandate concerning what employee activities it should investigate.

FIGURE 3

**Sources of Employee Investigations
Opened in Fiscal Year 2000–01**



Special Investigations has an unclear mandate concerning what it should investigate. Its written policy says it is responsible for investigating all cases of employee misconduct but does not define *misconduct*. Special Investigations might rely on state law, which dictates standards of conduct for employees, defining *misconduct* to include offenses such as dishonesty, immorality, misuse of state property, and inexcusable absence without leave.

Contrary to Special Investigations' written policy, its manager stated that it only investigates criminal misconduct, a position somewhat supported by a departmental directive issued in 1999 requiring that all allegations of criminal activity be referred to Special Investigations for review. However, Motor Vehicles' Zero Tolerance Policy on Employee Fraud or Dishonesty provides another view of Special Investigations' jurisdiction. This policy, released in 1997 and re-released by the current director in 2000, states that any act of fraud or dishonesty by an employee must be reported immediately, but either to a supervisor or directly to Special Investigations. The policy also leaves the definition of fraudulent or dishonest acts to the discretion of individual employees. Motor Vehicles' Supervisor's Guide to Employee Discipline provides yet another set of criteria for supervisors to reference when deciding whether certain employee activities, such as information security violations, should be referred to Special Investigations. According to this guide, supervisors are

not required to refer all potential criminal activity to Special Investigations. For example, supervisors use their judgment on whether to report incidents of unauthorized access to an employee's computer by another employee. This guidance conflicts with Special Investigations' written policy to investigate all cases of employee misconduct and with the departmental directive issued in 1999 requiring that all allegations of criminal activity be referred to Special Investigations.

Because Motor Vehicles lacks a comprehensive policy that clearly and consistently defines the types of activities that should be referred to Special Investigations, employees and managers must sift through conflicting policies and decide on their own which one applies to each case of employee misconduct. This discretion results in a lack of consistency in the types of activities that employees, managers, and regional administrators forward to Special Investigations. For example, we found that most regional administrators have chosen not to send all potential employee fraud activity directly to Special Investigations. Seven of the eight regional administrators require staff in their region to submit all potential employee fraud activities directly to them instead of Special Investigations for review. The administrators then determine if sufficient documentation exists to support a complaint. If a complaint is found to be either unsupported or invalid, the administrators do not forward it to Special Investigations but keep it on file and refer to it if similar complaints arise against the same employee. Only one regional administrator submits all potential employee fraud activity to Special Investigations. This inconsistent treatment may explain why Special Investigations' 18 employees have only opened 138 cases, fewer than 8 per employee, during fiscal year 2000–01.

Most of Motor Vehicles' regional administrators have chosen not to send all potential employee fraud activity directly to Special Investigations for review.

RECOMMENDATIONS

To increase its effectiveness in preventing fraud, assisting victims, and helping to prosecute wrongdoers, Investigations should take these actions:

- Establish procedures to more effectively manage its complaints and track accurate data. These procedures should cover, at a minimum, logging a complaint on receipt, promptly sending an acknowledgment letter to the complainant, prioritizing and assigning complaints, and deadlines for completing the investigation and reporting the results.

- Evaluate the feasibility of upgrading the case management database so that field offices can share data.
- Evaluate the feasibility of establishing a database that will allow it to provide better statistical data on fraudulent driver license and ID card use and identity theft.
- Evaluate the staffing needs of its branches and units.
- Establish a clear policy that identifies Special Investigations' role in investigating employee misconduct; defines such misconduct; and clarifies how employees, managers, and regional administrators are to report employee misconduct.

We conducted this review under the authority vested in the California State Auditor by Section 8543 et seq. of the California Government Code and according to generally accepted government auditing standards. We limited our review to those areas specified in the audit scope section of this report.

Respectfully submitted,



ELAINE M. HOWLE
State Auditor

Date: September 27, 2001

Staff: Joanne Quarles, Audit Principal, CPA
Michael Tilden, CPA
Matt Espenshade
Tony Nevarez
Karen R. Peterson
Amari B. Watkins
David Yorkowitz

Blank page inserted for reproduction purposes only.

Agency's comments provided as text only.

Business, Transportation and Housing Agency
Maria Contreras-Sweet, Secretary
980 9th Street, Suite 2450
Sacramento, California 95814

September 17, 2001

Elaine M. Howle*
State Auditor
Bureau of State Audits
555 Capitol Mall, Suite 300
Sacramento, CA 95814

Dear Ms. Howle:

Attached is the Department of Motor Vehicles' (Department) response to your draft audit report, *Department of Motor Vehicles: Although Unable to Measure the Extent of Identity Fraud and the Effect of Recent Reforms, It Should Improve Its Technology, Procedures, and Staffing Further* (#2001-103). As indicated in its response, the Department agrees with all the recommendations made in the draft report.

As you know, the Business, Transportation and Housing Agency (Agency) and the Department previously recognized the need for improvements in preventing identity theft and, in October of last year, began implementing a number of reforms. We are grateful for your additional ideas and, in fact, the Department has already begun working on some of the issues for which you made recommendations, such as training field representatives in ways to improve the quality of finger images. Most of the other recommendations, including those for various studies and evaluations, improved training, and improved controls, will be implemented over the next several months. For those recommendations involving the use of current technology and requiring additional funding from the Legislature, the Agency and the Department appreciate your support.

The Agency plans to work with the Department to address the many issues covered by this audit, and will support its efforts to make needed improvements.

*California State Auditor's comments begin on page 65.

Elaine M. Howle
September 17, 2001
Page 2

Thank you for the opportunity to respond to your audit. If you need additional information, please do not hesitate to contact me, or Michael Tritz, Chief of the Agency's Office of Internal Audits, at (916) 324-7517.

Sincerely,

(Signed by: Maria Contreras-Sweet)

MARIA CONTRERAS-SWEET
Secretary

Attachment

OFFICE OF THE DIRECTOR
DEPARTMENT OF MOTOR VEHICLES
P. O. BOX 932328
SACRAMENTO, CA 94232-3280

September 14, 2001

Maria Contreras-Sweet, Secretary
Business, Transportation and Housing Agency
980 - 9th Street, Suite 2450
Sacramento, CA 95814

Dear Secretary Contreras-Sweet:

Attached is our response to the Bureau of State Audits' (BSA) draft audit report regarding the procedures used by the Department of Motor Vehicles (DMV) to issue driver licenses. This audit was requested by the Joint Legislative Audit Committee, in response to a request from Senator Betty Karnette in January of this year.

On behalf of my entire department, I would like to acknowledge the high level of courtesy and cooperation we received from Joanne Quarles and her staff from BSA. From the beginning, they established an atmosphere of respect and trust, and created positive working relationships with all of the various staff they interacted with during the audit. Because of the tone they set at the outset, this audit proved to be a cooperative effort between BSA and DMV.

DMV is concerned about the title of this report, i.e., "Department of Motor Vehicles: Although Unable to Measure the Extent of Identity Fraud and the Effect of Recent Reforms, It Should Improve Its Technology, Procedures, and Staffing Further." While we acknowledge that some of this information is difficult, if not impossible, to quantify, we do have some data in this area, and are working on better performance measures. We do not believe the title of the draft report accurately reflects our overall ability to quantify the impact of fraud reforms, and could create a negative perception that is not supported by the narrative of the report, or the recommendations themselves.

①

The draft report is divided into two chapters. Chapter One focuses on the prevention of the issuance of fraudulent driver license and identification (DL/ID) cards, and Chapter Two focuses on improvements to our Investigations and Audits Division. There are a total of 16 recommendations in the draft report; 11 in Chapter One and five in Chapter Two.

Maria Contreras-Sweet, Secretary
September 14, 2001
Page 2

We are in agreement with all 16 of the recommendations. In fact, we had already identified many issues, including staffing, and had begun work on them.

As I promised during the fraud hearings in Long Beach during November 2000, DMV will continue to improve our ability to prevent the issuance of fraudulent documents. We recognize the critical role the DL/ID card plays in society, and it is my personal goal to eliminate this problem entirely. We certainly appreciate BSA's recommendation that the Legislature reevaluate its decision to eliminate the Governor's funding proposal for a biometrics system, and appreciate your support of this effort.

If your staff have any questions regarding any of our responses or the information provided, they may contact Sue Larson, Chief of the Program and Policy Development Branch in the Licensing Operations Division, at (916) 657-7634.

Sincerely,

(Signed by: Ed Snyder for)

STEVEN GOURLEY
Director

Attachment

ISSUE MEMORANDUM

TO: MARIA CONTRERAS-SWEET, Secretary
Business, Transportation and Housing Agency

FROM: STEVEN GOURLEY, Director
Department of Motor Vehicles

PREPARED BY: John McClellan, Deputy Director
Licensing Operations Division
(916) 657-6534 FAX: (916) 657-6261
E-mail: jmccllellan@dmv.ca.gov

DATE: September 14, 2001

SUBJECT: Bureau of State Audits Report: "Department of Motor Vehicles: Although Unable to Measure the Extent of Identity Fraud and the Effect of Recent Reforms, It Should Improve Its Technology, Procedures, and Staffing Further"

<u>For Use by Department</u>	<u>For Use by Agency</u>
<input type="checkbox"/> Request for Approval	<input type="checkbox"/> Reply Directly to Correspondent
<input type="checkbox"/> Request for Discussion	<input type="checkbox"/> Prepare Letter/Memo for Director's Signature
<input checked="" type="checkbox"/> For Secretary's Information	<input type="checkbox"/> Prepare Letter/Memo for Agency Secretary's Signature
<input type="checkbox"/> For Secretary's Signature	<input type="checkbox"/> Prepare Letter/Memo for Agency Staff Director's Signature
<input type="checkbox"/> Responding to Agency Request	<input type="checkbox"/> Prepare Letter/Memo for Agency Deputy/Assistant Secretary's Signature

AGENCY REFERENCE NUMBER:

TIME FACTOR:

This response is due to the Bureau of State Audits by 5:00 p.m. on Monday, September 17, 2001.

SUMMARY:

After the hearing in Long Beach in November 2000, Senator Betty Karnette requested that the Joint Legislative Audit Committee conduct an audit "to examine the procedures used by the Department of Motor Vehicles to issue drivers' licenses." Subsequently, at the direction of the Joint Legislative Audit Committee, the Bureau of State Audits (BSA) commenced this audit in March, 2001.

① The recommendations are repeated in this document, in bold text, along with our individual responses. We agree with all 16 recommendations, and had in fact already identified many issues, including staffing, and had begun work on them. We do take exception with the title of the report, and the associated narrative regarding our ability to quantify the impact of fraud reforms. The title is misleading and could create a negative perception that is not supported by the narrative of the report, or the recommendations themselves.

This is our initial response to the 16 recommendations. As required, the Department of Motor Vehicles (DMV) will provide three updates to these recommendations; the first at two months, the second at six months, and the final at the end of one year.

DISCUSSION/PRO-CON ARGUMENTS:

Recommendations:

The Bureau of State Audits (BSA) has made the following 16 recommendations (BSA recommendations are in bold):

If recent reforms prove ineffective, the Legislature should reconsider funding to support Motor Vehicles' upgrade of its finger imaging technology. If it chooses to fund the upgrade, the Legislature should consider protecting against unauthorized dissemination of finger images by limiting access to Motor Vehicles' imaging data to only those entities the Legislature finds have a legitimate interest in protecting the public, such as state and local law enforcement agencies. It should also consider imposing criminal sanctions for the unauthorized use of the data.

DMV agrees, and believes that funding for upgrading the current finger imaging technology should be allocated to the department irrespective of the current reforms. Although the current reforms are designed to prevent perpetrators from obtaining illegal driver license and identification (DL/ID) cards, these policies and procedures require manual intervention. With the use of biometrics to electronically verify an individual's identity, consistent and reliable technology will greatly improve DMV's identity verification process.

Various testimony provided at the Senate Transportation Committee hearing being held in Long Beach on November 16, 2000 (which included Senator Joseph Dunn, DMV Director Steven Gourley, and law enforcement officials) indicated that the use of biometrics should be implemented to significantly deter identity theft.

Earlier this year, DMV initiated plans to develop an automated solution to address DL/ID card fraud. This was in support of the Governor's FY 2001-2002 Budget that proposed \$7.7 million for biometric verification to address driver license fraud. Subsequently, the Senate Budget Bill (SB 75) Hearing deleted the funding while the Assembly Budget Bill (AB 95) proposed \$350,000 for a

consultant to develop a timeline, estimate costs, evaluate biometric identification processes, and develop a Feasibility Study Report. A subsequent Legislative Budget Hearing deleted all funding related to this effort. Despite the elimination of funding, DMV is proceeding with the necessary steps to develop a Feasibility Study Report using internal funds. If funds are approved by the Legislature, DMV intends to move forward with implementation of an automated identification verification solution.

DMV is involved with two other efforts related to biometrics:

- The thumbprint pilot with the California Department of Justice (DOJ) will test the feasibility of using DMV thumbprints with DOJ's automated fingerprint identification system to identify a person with multiple DL/IDs and assess the readability of prints in an automated environment. A sample of 300,000 DL/ID numbers, along with corresponding fingerprint images, were sent to DOJ. The results of this pilot are pending; however, we hope this will help determine the readability of our existing fingerprint images and the extent of fraud in our records.
- The Federal Motor Carrier Safety Administration Biometric Demonstration Project will determine the feasibility of using automated fingerprint identification and facial recognition technology to accurately identify commercial driver license (CDL) holders. In addition to California, Georgia and West Virginia are also participating in this project that is being funded through a federal grant.

DMV will continue to uphold the law and protect the images from unauthorized access or use. It has always been DMV's position that biometrics should only be shared with those entities entitled to receive the information.

Additionally, if the Legislature approves the use of finger imaging, it should consider directing Motor Vehicles to establish controls that protect the privacy of California citizens. More specifically, the Legislature should consider directing Motor Vehicles to establish protocols that ensure the following:

DMV agrees with this recommendation. DMV already has numerous stringent controls in place to secure the massive amounts of confidential data, e.g., thumbprint and residence address, that it maintains. DMV has suggested the following for implementation if a biometrics program is funded.

◆ **That controls exist to prevent the improper disclosure of finger images.**

DMV agrees with this recommendation and already controls its image database. If this program is funded, DMV will:

- Limit the access and authorizations used to collect, or share, biometrics within the boundaries authorized by the California Vehicle Code (CVC).
- Automate the biometric process as much as possible to prevent human intervention.
- Not allow the applicant or DMV staff to circumvent the capture, comparison and storage processes in order to initiate or perpetuate undetected fraudulent DL/ID transactions.
- Assure that the biometric data will be in the control of and owned by DMV.
- Assure that appropriate encryption is used during data transmission and storage.

- Assure that only authorized DMV individuals are capable of controlling access, adding, correcting, and deleting biometric data.

◆ **That the physical documents supporting the data are kept in a secure area.**

DMV agrees that all data be kept in a secure area. Currently, thumb or finger images are captured and stored electronically requiring no "physical document" to be maintained. The thumb or finger images will be kept in a secure area by prohibiting access to images except those with appropriate authorization and need.

◆ **That sufficient firewalls and other electronic security measures are used to secure the computer network from "hackers" and criminal interests.**

DMV agrees that electronic security measures should be used to secure the computer network. In addition to meeting the security policies and requirements as defined in DMV's Information Security Policy manual and the state Architecture and Security Requirements for eGovernment, security measures will achieve the following:

- The system configuration minimizes vulnerabilities.
- The system configuration has intrusion prevention tools to proactively monitor, identify, report, and respond to unauthorized attempts to access, modify, compromise, and remove the biometric identification system from service, or internal tampering or collusion.
- The system security includes password protection for access with different levels of control over the data.
- Steps are taken to ensure the proposed system satisfies the security requirements outlined in State Administrative Manual 4840 - 4845, as well as ensure adequate separation of duties.
- Data integrity is not compromised by new applications or interfaces, including not allowing biometric templates to be altered.
- Effective data controls exist to protect the privacy of customer's information as outlined in CVC 1808 and the Driver's Privacy Protection Act of 1994.

◆ **That access to the database is limited and an "audit trail" exists to identify users of the data.**

DMV agrees that access to the database be limited and that "audit trails" exist. In addition to limiting access to the database to authorized users and maintaining an audit trail to identify those users, the biometrics system must provide for a standard and ad hoc audit trail reports, to be kept either electronically or in hard copy. The audit trail of the users of the system must also track use and efficiency of the processes, and, at a minimum, provide user identification, date, time, office identification, workstation identification, and type of DL/ID transaction.

To further improve its existing controls and reduce field office waiting times, Motor Vehicles should:

Train its field representatives to capture good finger images, not allowing them to bypass obtaining readable customer images without prior approval from their managers.

We agree with the recommendation and have already identified it as an issue. In an ongoing effort to reduce fraud, it is extremely important that an emphasis is placed on improving the quality of the thumbprints captured during the photo process. To address this issue, in July 2001, DMV began working with the photo capture station vendor and has identified a new hand position and other methods to capture better prints which will ultimately reduce the number of attempts and/or overrides. By the end of September 2001, Field Office Managers will be provided with detailed information and instructions of these new methods. All field office employees will be scheduled to be trained in this enhanced thumbprint capture process by November 2001. To further emphasize the training, a video outlining these new methods has been developed and will be released to all field offices.

2

On August 1, 2001, approval was granted to implement a pilot effort in two field offices to determine the feasibility and benefits of requiring a supervisor's approval for any override. An initial survey will be completed to document the current number of and reasons for thumbprint overrides. The data will be analyzed to determine any gaps in current training, procedures or equipment use. Employees will then be specially trained as described above. Other surveys will be conducted in the same two field offices after the training is completed. The data from the surveys will be analyzed and the results of the pilot will be evaluated to determine if supervisory approval for overrides or additional training is necessary. We anticipate this pilot and evaluation will be completed in December 2001.

Establish mechanisms to measure the effectiveness of its recent and future reforms.

DMV agrees that information to establish quantitative data on fraud reforms is important to establish the degree of effectiveness. As initiatives are being developed, consideration is being given to ways in which historical and future data can be collected and stored, to quantify the changes due to a reform. By establishing fraud task forces and including members of privacy rights groups, financial institutions and law enforcement, we are better able to determine the types of fraud perpetrated and the ways in which this fraud exists. With this information, DMV can tailor its data collection in order to effectively measure changes in several different areas.

The department has processes and measurements in place to measure the effectiveness of the fraud reforms implemented in October 2000, and January 2001. The following summarizes the types of data we are able to provide:

1

Since we have been retrieving the applicant's prior photo, we have data to show:

- The number of fraudulent DL/ID cards that were prevented from being issued.
- The number of applications containing fraudulent activity that were prevented from being issued before the true owner was even aware of the problem.

Since requiring that two people verify the legal presence documents, we have:

- Seen a decrease in employee fraud.
- Detected thousands of documents that appear to be counterfeit or fraudulent.

Since implementing the toll free identity theft phone line, we have data to show:

③

- We have assisted thousands of customers with their concerns regarding their DMV record.
- We have identified hundreds of records that had previously been compromised.

Continue to work on its plan to electronically reconcile system transactions against applications sent for microfilming at headquarters to ensure that an application supports each transaction. Further, field office managers should ensure that field representatives enter barcodes on all paper applications before sending them to headquarters.

We agree with the above recommendations. The Electronic Oversight Branch is working with the Field Operations Division (FOD) and the Information Systems Division to identify those applications where a barcode was not entered and implement improved processes to ensure that every transaction is supported by a microfilmed application. This entails compliance, procedural and programming issues, as well as installation of adequate barcode scanning equipment. We will have a plan in place within six months.

Instruct Fraud Analysis to conduct a study to determine whether it would be beneficial to compare new photos for those existing customers obtaining any temporary license, driver license, or ID card to the history of photos contained in Motor Vehicles' database to verify that it is the same person.

④

DMV agrees with this recommendation. Since October 2000, we have been retrieving the applicant's prior photo unless the applicant has specified valid identification in their possession. This recommendation targets those licenses issued to customers who present acceptable documents and, therefore, have photo retrieval waived. Within the next 60 days, the department will undertake a study to:

- Identify all DL/ID cards that were issued within the last six months with a new photograph having been taken.
- Work with the DMV Research and Development Branch to establish an appropriate statistical sample of these DL/IDs.
- Review the photographic history of these records to determine if there are any indications of fraud.
- Evaluate any records that contain fraud to determine how the fraud may have occurred.

This study will determine the benefit of comparing new photos for those existing customers obtaining any temporary license, driver license, or ID card to the history of photos contained in Motor Vehicles' database to verify that it is the same person.

Establish deadlines for staff to address all of the Anti-Fraud Task Force recommendations and conduct a timely evaluation of these recommendations' merits.

As reported by the California State Auditor, the DMV has not yet evaluated all of the recommendations of the Anti-Fraud Task Force (task force). We agree with the importance of a timely evaluation of the merits of each of the suggestions. This response provides information on the department's plan to ensure all recommendations are addressed.

The department is focused on eliminating fraud in all its services and products while continuing its core business processes and providing good customer service. Due to the need to use our resources as efficiently as possible, all anti-fraud suggestions were prioritized to focus efforts on those suggestions considered to have the biggest impact.

Late last year, the task force provided recommendations related to driver license, ID card, and employee fraud. The department reviewed those recommendations and identified other concerns. A group of high-level managers from throughout the department organized, categorized and subcategorized the recommendations to determine overall departmental initiatives and priorities. Those suggestions that seemed possible to evaluate and implement within six months were identified as "Quick Hits"; the other recommendations were organized into one of eight initiatives, each addressing a particular area of fraud.

Analysis and implementation of the "Quick Hits" have been given first priority since these suggestions could be quickly implemented (within six months). Many of the task force recommendations were identified as "Quick Hits".

Team Leads were assigned to each of the eight initiatives. The Leads reviewed the recommendations in their initiatives and prioritized the suggestions for completion of detailed analysis and evaluation of recommendations. The potential time frame for implementation was assessed first. Recommendations were categorized as short-, medium-, or long-term:

- Short-term - Potentially completed by June 2002, requiring no legislation nor additional funding.
- Medium-term - Potentially completed by June 2003, possibly requiring legislation, additional funding, and/or programming.
- Long-term - Potentially completed after June 2003, requiring legislation, additional funding, and/or major new technology.

Recommendations were again categorized using the following criteria to rank the suggestions on their potential impact on fraud, assessing factors such as whether the idea would:

- Improve document integrity;
- Discourage employees and/or customers from attempting fraudulent acts;
- Help to measure the incidence of fraud;
- Reduce the opportunity for fraudulent transactions;
- Affect a significant number of transactions; and/or
- All or some of the above.

Using these criteria and the time frame model, due dates were established for completion of analysis of the first group of recommendations. Most of the task force recommendations were identified in this first round of analysis, which will be completed by the end of 2001. Other task force recommendations will be evaluated in the next phase and due dates for analysis will be assigned by January 2002. It must be noted that none of the recommendations have been eliminated or discarded. Resources are being applied initially where the strongest impact on fraud can be achieved.

Twelve of the recommendations have been implemented, and six are in progress. Eleven recommendations have been identified to need legislation; seventeen need funding, resources, and/or a

detailed technology needs study. As noted in the auditor's report, some actions are outside of DMV's control. These recommendations will be addressed with the appropriate entities.

While the department welcomes any and all suggestions to prevent, detect, and/or deter fraud, priority of our efforts was established to ensure that immediate action was taken. Staff from all programs are actively engaged in the review, analysis and/or implementation of the task force recommendations, supported by other employees, as needed.

The Director has determined DMV's anti-fraud efforts must be given the highest priority and continued until all feasible actions have been taken. To show the Director's commitment, he named two executive managers as the sponsors of the department's anti-fraud efforts with primary responsibility for review and oversight.

Continue its efforts to decrease field office waiting times by installing the additional queuing systems and posting real time data to its Internet site. Also, determine if it needs to install more video capture stations for photo retrieval in the field offices. Finally, it should complete a staffing analysis to assess the impact that the recent reforms have had on its ability to carry out its procedures.

We agree with the recommendations. As noted within the report, the department has already secured authority and funding for its Queuing System Expansion project, which will install queuing systems in an additional 66 field offices over the next two fiscal years. In addition, the eight regional offices will be equipped with queuing monitoring systems, providing region administrators a real time view of wait times and the number of customers in an office at any given time. This will result in queuing systems in 102 of our busiest offices at the Grades III, IV and V levels. Once all systems are installed, our long term plans include evaluating the feasibility and benefit of continuing installations in the remaining offices, and eventually posting real time wait data to our internal intranet and/or the department's internet web site.

Regarding the recommendation that we determine if the department needs to install more video capture stations, it should be noted that earlier this year the department did secure and install 35 additional video capture stations to allow for additional photo retrievals in metropolitan field offices. We now have a total of 290 plus video capture stations in our field offices. However, for each video capture station installed, one workstation is eliminated, minimizing the number of available windows in the office where transactions may be processed. Therefore, the department will pursue implementation of additional photo retrieval capability by other means. The terminal replacement project will provide "thin-client" terminals to replace the current "dumb" terminals utilized at each workstation. These "thin-client" terminals will provide additional capabilities that are not available with the current, obsolete equipment. In lieu of additional video *capture* stations, we will develop the appropriate programming, software and cabling to utilize these new "thin-client" terminals to retrieve photos at each workstation, negating the need for additional video capture stations.

6

We agree a staffing analysis should be undertaken. As indicated in the report, the new photo retrieval procedure resulted in approval for an additional 21 positions to staff the 35 video capture stations. An initial analysis of the new fraud procedures for original applications estimates the need for an additional 70 positions in our field offices, based on assumptions that can now be validated. We will complete the analysis to validate and/or modify that resource requirement over

the next six months. It should also be noted that the department is currently undertaking a demographics study that may provide additional justification to assist in allocating resources.

Instruct its Field Operations management to meet with field office managers to reiterate training expectations and monitor them for compliance with Field Operations' training goals.

We agree with this recommendation, and will reiterate training expectations for the fraud document detection classes. It will be necessary to manually monitor compliance until the department's training databases are improved or replaced to provide accurate information. We will have a report of the personnel trained by reporting unit location within 60 days, and will keep that report updated manually, and share the results with region and office managers as part of our ongoing commitment to provide appropriate training.

Correct training database errors and modify the Administrative Services' training database to allow users to view and sort employees' attendance at the fraudulent document detection training by reporting unit location.

We agree with this recommendation. There are two separate databases maintained relative to fraudulent document training: one in the Investigations and Audits Division (IAD) and one in the Administrative Services Division. There are discrepancies between the two that we will analyze and take corrective measures to resolve. As to the issue of viewing and sorting employee attendance by reporting unit location, we intend to work with all impacted divisions, most notably FOD, to implement this enhancement. We also plan to work with these divisions to determine any other enhancements to these systems that would make the data more relevant and useful to them.

Continue to communicate with trainers and supervisors regarding Motor Vehicles' commitment to standardization and uniformity. Determine if Investigations needs additional funding to implement short-, mid-, and long-term goals for improving its training program.

DMV agrees with this recommendation. A meeting with all of the trainers was held on September 6, 2001, to emphasize the need for standardization and uniformity. Additionally, within the next 60 days the department will establish a plan for the continuing operation of this training program. This plan will include: the purpose, the need, the scope of the training provided, the resources required (both trainer and materials), and established goals for this program. Staff will ensure that the needs identified in this plan are available for the next budget cycle to ensure that additional resources can be requested through a Budget Change Proposal.

To increase its effectiveness in preventing fraud, assisting victims, and assisting in the prosecution of wrongdoers, the Department of Motor Vehicles Investigations and Audits Division should take these actions:

Establish procedures to more effectively manage its complaints and track accurate data. These procedures should cover, at a minimum, the logging of a complaint upon receipt, a prompt acknowledgment letter sent out to the complainant, procedures for prioritizing and assigning complaints, and deadlines for completing the investigation and reporting the results.

DMV agrees with this recommendation. The current IAD staff will immediately begin development of the necessary procedures to manage its complaints and track accurate data. Within the next six months, it is anticipated that appointments will be made for the two vacant management positions within IAD. Once appointed, this management team will evaluate these procedures and establish a mechanism to ensure accountability.

Evaluate the feasibility of upgrading its case management database so that field offices can share data.

DMV agrees with this recommendation. Within the next six months, IAD will undertake a feasibility study to determine case management needs, identify alternative solutions, and recommend an appropriate replacement database that will allow for field offices to share data. Divisional staff will ensure that the results of this study are available for the next budget cycle to ensure that additional funding can be requested through a Budget Change Proposal, if necessary.

Evaluate the feasibility of establishing a database that will allow it to provide better statistical data on fraudulent driver license and ID card use and identity theft.

DMV agrees with this recommendation. Within the next six months, IAD will undertake a feasibility study to determine an appropriate method to gather better statistical data on fraudulent driver license and ID card use and identity theft. Divisional staff will ensure that the results of this study are available for the next budget cycle to ensure that additional funding can be requested through a Budget Change Proposal, if necessary.

Evaluate the staffing needs of its branches and units.

DMV agrees with this recommendation. Within the next six months, IAD will undertake a study to determine the staffing needs of each of its branches and units. Divisional staff will ensure that the results of this study are available for the next budget cycle to ensure that additional positions can be requested through a Budget Change Proposal.

The peace officer powers of the investigators are defined in Section 1655 CVC. This section defines the powers as ". . . the investigators of the department . . . shall have the powers of peace officers for the purpose of enforcing those provisions of law now and hereafter committed to the administration of the department or enforcing the law on premises occupied by the department."

7 While the audit report speaks of the responsibilities of the Field Investigations Branch related to enforcing the law on DMV's premises, it fails to identify many other responsibilities, including investigations of:

- DL/ID card fraud, counterfeit, and thefts.
- Vehicle Registration and Title fraud, counterfeiting, and theft.
- Odometer fraud.
- Stolen vehicles and vessels.
- Registration service fraud.
- Unlicensed vehicle sales.

- Occupational licensing fraud, theft, misrepresentation and advertising fraud.
- Fraud related to the department's information.

Investigators support DMV in all of these cases by investigating and assisting in the prosecution of individuals, employees, licensees, information services requesters and business partners suspected of violating motor vehicle, criminal, civil and administrative codes and regulations.

In addition, there are two other Branches in the Investigations and Audits Division not mentioned in the audit report-Information Protection Services and Internal Audits. Staff from these Branches support the department by providing information technology security, risk analysis, disaster recovery planning, and review of accounting and administrative controls.

Establish a clear policy that identifies Special Investigations' role in investigating employee misconduct, defines such misconduct, and clarifies how employees, managers, and regional administrators are to report employee misconduct.

We agree with the recommendation. There is a conflict in the way that the Investigation's policy and procedures are written. Within the next sixty days, the policy and procedures will be reviewed and re-written to establish a clear policy on reporting employee misconduct cases and what Special Investigations' role will be in investigating the misconduct.

EFFECT ON EXISTING LAW:

N/A

ESTIMATED COST:

N/A

RECOMMENDATION:

Approve the report.

APPROVED:

(Signed by: Ed Snyder for)

STEVEN GOURLEY

Director

Department of Motor Vehicles

Blank page inserted for reproduction purposes only.

COMMENTS

California State Auditor's Comments on the Response From the Department of Motor Vehicles

To provide clarity and perspective, we are commenting on the Department of Motor Vehicles' (Motor Vehicles) response to our audit report. The numbers below correspond to the numbers we placed in the margins of Motor Vehicles' response.

- ① We disagree with Motor Vehicles and believe that the title of our report is supported by relevant, sufficient evidence, and is consistent with the conclusions reached in our report. Motor Vehicles cannot measure the impact of its recent reforms. Specifically, as we state on page 23, although its Driver License and Fraud Analysis Unit (Fraud Analysis) tracks potential fraudulent applications, when it forwards them to the Field Investigations Branch (Field Investigations) they are pooled with cases originating from other sources. As a result, Motor Vehicles cannot identify the number of confirmed fraudulent applications resulting only from the photo retrieval process. Also, as we state on pages 23 and 24, Motor Vehicles cannot measure the effect of its new secondary verification procedure because it is hard to determine how many customers with potentially fraudulent documents were deterred, it changed its procedure for reviewing those applications that field representatives flag for further review, and its field investigators do not track the number of cases they receive relating to this procedure. Therefore, Motor Vehicles has no way of knowing if the apparent increases in fraudulent applications are based solely on the second employee's verification of documents. Finally, as we state on pages 22 and 23, Motor Vehicles cannot quantify how many customers with questionable Social Security information were unsuccessful in obtaining fraudulent driver licenses or identification cards (ID cards) because it has chosen not to pursue unresolved requests that it submits to the federal Social Security Administration. Consequently, these findings have led us to conclude that Motor Vehicles is unable to measure the effect of its recent reforms.

- ② While we are pleased that Motor Vehicles considers it important to improve the quality of finger images it captures, we believe it is overstating the extent of its efforts. Specifically, we found that the discussions with its vendor and instructions given to its staff concerning other methods to use when capturing prints were merely a reiteration of fundamental techniques such as cleaning the glass plate and providing towelettes for customers to clean excess oils or lotions from their fingers. Moreover, the new hand position that its vendor suggests is simply having customers approach the finger-image device with their palm open instead of closed to help Motor Vehicles field representatives capture better prints.
- ③ We disagree with Motor Vehicles characterization of its consumer fraud hotline data. Although Motor Vehicles can identify the number of calls it receives where consumers suspect their driver licenses or ID cards have been compromised, it cannot identify the number of calls that result in a confirmation that the consumer's documents have actually been compromised. Specifically, as we state on page 43, Fraud Analysis receives calls from the hotline. These calls, similar to the potential fraudulent applications identified by Motor Vehicles' new photo retrieval process, are sent to Field Investigations and pooled with cases originating from other sources.
- ④ Motor Vehicles has misinterpreted our recommendation. As we state on pages 24 and 25, there is some risk that an employee could assist a customer in assuming the identity of another individual because Motor Vehicles does not require two employees to validate existing customers' photo retrievals when issuing temporary licenses, driver licenses, or ID cards. Our recommendation is aimed at reducing this risk.
- ⑤ Motor Vehicles' status of recommendations differs from the status we report on page 26 because it includes action taken on other fraud-related issues that its Anti-Fraud Task Force did not specifically address.
- ⑥ Although Motor Vehicles' decision to develop appropriate programming, software and cabling to use new "thin-client" terminals to retrieve photos at each workstation appears to address its concern of minimizing any delays in customer service, this project is long-term. Specifically, Motor Vehicles does not expect to make "thin-client" terminals available in all of its field offices until June 30, 2003. Moreover, Motor Vehicles has yet to pursue funding for the software and cabling that will allow these

terminals to retrieve and display photos. Therefore, this project does not address Motor Vehicles apparent immediate need for improved photo retrieval access that we discuss on page 30.

- ⑦ We recognize that Field Investigations has many other responsibilities. However, as we state on pages 9 and 10, the Joint Legislative Audit Committee asked us to assess Motor Vehicles' procedures for investigating reports of fraudulent driver licenses. Any other Field Investigations' responsibilities are outside the scope of this audit.

cc: Members of the Legislature
Office of the Lieutenant Governor
Milton Marks Commission on California State
Government Organization and Economy
Department of Finance
Attorney General
State Controller
State Treasurer
Legislative Analyst
Senate Office of Research
California Research Bureau
Capitol Press